DISTRIBUTION OF ZETA ZEROES FOR ABELIAN COVERS OF ALGEBRAIC CURVES OVER A FINITE FIELD

MAOSHENG XIONG

Abstract. For a function field k over a finite field with $\mathbb{F}_q$ as the field of constant, and a finite abelian group G whose exponent is divisible by $q-1$, we study the distribution of zeta zeroes for a random G-extension of k, ordered by the degree of conductors. We prove that when the degree goes to infinity, the number of zeta zeroes lying in a prescribed arc is uniformly distributed and the variance follows a Gaussian distribution.

1. Introduction

There has been some interest recently in statistics of zeroes of zeta functions for curves over a finite field $\mathbb{F}_q$. The fascinating theory of Katz and Sarnak ([9]) roughly states that as $q \to \infty$, the limiting distribution of zeroes of L-functions in a family of "geometric objects" defined over $\mathbb{F}_q$ is the same as that of eigenvalues of random matrices in certain monodromy groups. Here, however, the condition $q \to \infty$ is necessary as the argument depends on Deligne's equidistribution theorem ([6]). One question hence remains: what happens if the field size q is fixed and other parameters go to infinity?

2000 *Mathematics Subject Classification.* 11G20,11T55,11M38.

Key words and phrases. Zeta functions of curves, Class field theory, Gaussian distribution.

The author was supported by the Research Grants Council of Hong Kong under Project Nos. RGC606211 and DAG11SC02.

In this direction Faifman and Rudnick ([8]) studied statistics of zeroes of zeta functions for the family of hyperelliptic curves of genus g over $\mathbb{F}_q$. This is given explicitly by the affine model

$$C_f : y^2 = f(x), \tag{1}$$

where f runs over the set of monic square-free polynomials of degree $2g+2$. The zeta function of $C_f/\mathbb{F}_q$ has $2g$ zeroes, and by the Riemann Hypothesis for curves ([17]), all of them lie on a circle of radius $q^{-1/2}$. They proved that as $g \to \infty$, the number of such zeta angles inside a fixed interval $\mathbf{I} \subset (-1/2, 1/2)$ is asymptotically $2g|\mathbf{I}|$, here $|\mathbf{I}|$ is the length of $\mathbf{I}$, and the variance of this quantity as C_f varies in the family is a Gaussian distribution; moreover, the result holds for shrinking intervals as long as $2g|\mathbf{I}|$ tends to infinity. This family form the moduli space of hyperelliptic curves of a fixed genus on which the distribution result can be reformulated. This result is consistent with the random matrix model predicted by the theory of Katz and Sarnak when both g and q tend to infinity.

This beautiful work of Faifman and Rudnick was extended to the family of l-fold covers of the projective line ([21]), and more recently to the family of Artin-Schreier covers of the projective line ([4]), on which similar distribution results were obtained. The results can also be adapted to moduli spaces for these two families. Interested readers may refer to [21, 4] for details. In the same spirit with respect to other statistics, in particular, the distribution of the number of $\mathbb{F}_q$-points on a family of curves or similar statistics as $g \to \infty$, this is slightly easier, and distribution results have been obtained for quite a few families (see for example [1, 2, 3, 5, 7, 10, 11, 18]).

The above families of curves, as interesting and important as they are, could be interpreted in a different way. Let $k = \mathbb{F}_q(x)$ be the rational function field. Hyperelliptic curves C_f defined in (1) correspond to quadratic extensions $k(\sqrt{f(x)})$ of k with Galois group $\mathbb{Z}/2\mathbb{Z}$. Similarly l-fold covers of the projective line in [21] correspond to function field extensions of k with Galois group isomorphic to $\mathbb{Z}/l\mathbb{Z}$ (here $q \equiv 1 \pmod{l}$), and Artin-Schreier curves considered in [4] correspond to extensions of k with Galois group isomorphic to $\mathbb{Z}/p\mathbb{Z}$, where p is the characteristic of $\mathbb{F}_q$. Since the zeta function of a curve over $\mathbb{F}_q$ is the same as the zeta function of its function field ([13]), the results of [8, 21, 4] can be summarized as distribution of zeroes of zeta functions for function fields running over abelian extensions of k with the Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/l\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z}$ respectively. It is natural to investigate the question: how are the zeta zeros distributed as function fields run over abelian extensions of any function field with any fixed finite Galois group? Or in other words, how are the zeta zeros distributed for abelian covers of an algebraic curve over a finite field with a fixed Galois group?

From now on we fix an arbitrary function field k with field of constant $\mathbb{F}_q$ and a finite abelian group G. Define a G-extension of k to be a Galois extension $\mathbb{K}/k$ with an isomorphism $\phi_{\mathbb{K}} : \mathrm{Gal}(\mathbb{K}/k) \to G$. An isomorphism of two G-extensions $\mathbb{K}$ and $\mathbb{K}'$ is given by an isomorphism $\mathbb{K} \to \mathbb{K}'$ of k-algebras that respects the G-action on $\mathbb{K}$ and $\mathbb{K}'$. Let $E_G(k)$ be the set of isomorphism classes of G-extensions of k. For a G-extension $\mathbb{K}$, let $\mathrm{Cond}(\mathbb{K})$ be the conductor of $\mathbb{K}$ over k. For each positive integer d, we define

$$E_G(k,d) = \{\mathbb{K} \in E_G(k) : \deg_k \mathrm{Cond}(\mathbb{K}) = d\}. \tag{2}$$

It will be clear that this is a finite set, with $\#E_G(k,d) \to \infty$ as $d \to \infty$. We assign the uniform probability measure on $E_G(k,d)$.

We shall study the distribution of zeroes for the zeta function $\zeta_{\mathbb{K}}(s)$ as $\mathbb{K}$ runs over the set $E_G(k,d)$ under the limit $d \to \infty$. It is known that $(1-q^s)\,(1-q^{1-s})\,\zeta_{\mathbb{K}}(s)$ is a polynomial of degree $2g_{\mathbb{K}}$ in q^{-s}, where $g_{\mathbb{K}}$ is the genus of $\mathbb{K}$ and satisfies the Riemann hypothesis ([15]), so we may write

$$\zeta_{\mathbb{K}}(s) = \frac{\prod_{i=1}^{2g_{\mathbb{K}}} \left(1 - \sqrt{q} e(\theta_{\mathbb{K},i}) q^{-s}\right)}{(1-q^s)\,(1-q^{1-s})},$$

here $e(\alpha) = e^{2\pi i \alpha}$ and the angles satisfy $\{\theta_{\mathbb{K},i} : i\} \subset [-\frac{1}{2}, \frac{1}{2})$. Now we fix a subinterval $\mathbf{I} \subset (-\frac{1}{2}, \frac{1}{2})$, and for simplicity as in [8], we assume that $\mathbf{I}$ is symmetric around the origin. Define

$$N_{\mathbf{I}}(\mathbb{K}) = \#\left\{i : \theta_{\mathbb{K},i} \in \mathbf{I}\right\}.$$

We will study how the quantity $N_{\mathbf{I}}(\mathbb{K})$ is distributed as $\mathbb{K}$ runs over the set $E_G(k,d)$ with $d \to \infty$. We prove

Theorem 1. *Let k be a function field with field of constant $\mathbb{F}_q$ and G be a finite abelian group of order κ such that $q \equiv 1 \pmod{\exp(G)}$ where $\exp(G)$ is the exponent of G. Let $\mathbf{I} \subset \left(-\frac{1}{2}, \frac{1}{2}\right)$ be a symmetric subinterval and assume that $d|\mathbf{I}| \to \infty$ as $d \to \infty$ where $|\mathbf{I}|$ is the length of $\mathbf{I}$. Then for any real numbers a, b, we have*

$$\lim_{d\to\infty} \operatorname{Prob}_{E_G(k,d)} \left(a < \frac{N_{\mathbf{I}}(\mathbb{K}) - g_{\mathbb{K}}|\mathbf{I}|}{\sqrt{\frac{2(\kappa-1)}{\pi^2} \log(g_{\mathbb{K}}|\mathbf{I}|)}} < b \right) = \frac{1}{\sqrt{2\pi}} \int_a^b e^{-\frac{x^2}{2}}\, \mathrm{d}x\,.$$

We remark that the technical condition $q \equiv 1 \pmod{\exp(G)}$ effectively excludes Artin-Schreier extensions considered in [4]. As was shown in [4], even over the rational function field, the treatment of Artin-Schreier extensions is quite different from [8, 21], which means that to include such extensions in Theorem 1 might be technically complicated. We also remark that Theorem 1 is consistent with results in [8, 21, 4] when $\#G = 2, l \geq 3$ and p respectively.

As was noted in [21] and [4], there is a subtle structure, that is,

$$\zeta_{\mathbb{K}}(s) = \zeta_k(s) \prod_{1 \neq \rho \in \widehat{G}} L(k, \rho \circ \phi_{\mathbb{K}}, s),$$

where $L(k, \rho \circ \phi_{\mathbb{K}}, s)$ is the L-function with respect to a non-principal character ρ. Since each $L(k, \rho \circ \phi_{\mathbb{K}}, s)$ satisfies the Riemann hypothesis, it is more natural to study the distribution of zeroes of $L(k, \rho \circ \phi_{\mathbb{K}}, s)$ for a fixed ρ as $\mathbb{K}$ varies in $E_G(k, d)$. To be more precisely, for any non-principal character $\rho \in \widehat{G}$, it is known that each $L(k, \rho \circ \phi_{\mathbb{K}}, s)$ is a polynomial of degree say $m_{\rho,\mathbb{K}}$ in q^{-s} with constant term 1 and satisfies the Riemann hypothesis ([15]), so we may write

$$L(k, \rho \circ \phi_{\mathbb{K}}, s) = \prod_{i=1}^{m_{\rho,\mathbb{K}}} \left(1 - \sqrt{q} e(\theta_{\rho,\mathbb{K},i}) q^{-s}\right),$$

here $e(\alpha) = e^{2\pi i \alpha}$ and the angles satisfy $\{\theta_{\rho,\mathbb{K},i} : i\} \subset [-\frac{1}{2}, \frac{1}{2})$. The collection of zeta angles $\{\theta_{\rho,\mathbb{K},i} : 1 \leq i \leq m_{\rho,\mathbb{K}}\}$ for all the ρ's (together with zeros of $\zeta_k(s)$) gives all the zeros of $\zeta_{\mathbb{K}}(s)$. Now we fix a symmetric subinterval $\mathbf{I} \subset (-\frac{1}{2}, \frac{1}{2})$, and define

$$N_{\rho,\mathbf{I}}(\mathbb{K}) = \# \left\{ i : \theta_{\rho,\mathbb{K},i} \in \mathbf{I} \right\}.$$

We will investigate a more subtle question, that is, what is the joint distribution of the quantities $N_{\rho,\mathbf{I}}(\mathbb{K})$ for non-principal characters ρ when $\mathbb{K}$ runs over the set $E_G(k, d)$ as $d \to \infty$. Since clearly $N_{\rho,\mathbf{I}}(\mathbb{K}) = N_{\rho^{-1},\mathbf{I}}(\mathbb{K})$, from possibly two characters ρ, ρ^{-1} we only need to consider one of them. We prove

Theorem 2. *Let k be a function field with field of constant $\mathbb{F}_q$ and G be a finite abelian group such that $q \equiv 1 \pmod{\exp(G)}$ where $\exp(G)$ is the exponent of G. Let $\rho_i : G \to \mathbb{C}^*, 1 \leq i \leq t$ be distinct non-principal characters of G such that $\rho_i\rho_j \neq 1$ for any $i \neq j$. Let $\mathbf{I} \subset \left(-\frac{1}{2}, \frac{1}{2}\right)$ be a symmetric subinterval and assume that $d|\mathbf{I}| \to \infty$ as $d \to \infty$ where $|\mathbf{I}|$ is the length of $\mathbf{I}$. Then for any real numbers $a_i, b_i, 1 \leq i \leq l$, we have*

$$\lim_{d\to\infty} \mathrm{Prob}_{E_G(k,d)} \left(a_i < \frac{N_{\rho_i,\mathbf{I}}(\mathbb{K}) - m_{\rho_i,\mathbb{K}}|\mathbf{I}|}{\sqrt{\frac{r_{\rho_i}}{\pi^2}\log(m_{\rho_i,\mathbb{K}}|\mathbf{I}|)}} < b_i, \ \forall\, 1 \leq i \leq t \right) = \prod_{i=1}^{t} \frac{1}{\sqrt{2\pi}} \int_{a_i}^{b_i} e^{-\frac{x^2}{2}}\,\mathrm{d}x\,,$$

where

$$r_\rho = \begin{cases} 1 & : \quad \text{if the order of } \rho \text{ is } \geq 3; \\ 2 & : \quad \text{if the order of } \rho \text{ is } 2. \end{cases}$$

Remark. (a). Compared with Theorem 2, the number r_ρ is missing in [21, Theorem 1]. That was a typo. Actually the proof there was correct and clearly indicated that the factor 2 should be replaced by r_ρ, which depends on whether or not $\rho^2 = 1$. This is consistent with [8, 4].

(b). The family of G-extensions of k form the moduli space of abelian covers of an algebraic curve over $\mathbb{F}_q$ on which similar results as Theorems 1 and 2 can formulated...

(c). We count G-extensions of k by conductors (see the definition of $E_G(k, N)$ given in (2)). It might be more interesting to count G-extensions by discriminants, as discriminants determine the genus of the function fields (see the Riemann-Hurwitz formula ([15, Theorem 7.16])). However, this turns out to be more difficult, as already noted in [19] (see also [20]), and we are not able to do it here. We might pursue it in the future.

The paper is organized as follows. In Section 2, we collect several results which will be used later. In Sections 3-4, we analyze certain sums over a larger set $\widetilde{E}_G(k,d)$ (see the definition in (6)). This part is inspired by the paper [19]. In Section 5 we prove Theorem 1 for the set $\widetilde{E}_G(k,d)$ as $d \to \infty$. In the final section, Section 6, Theorem 1 on $E_G(k,d)$ is derived from the results on $\widetilde{E}_G(k,d)$, and Theorem 2 is also derived from Theorem 1.

2. Preliminaries

In this section we collect several results which will be used later. Interested readers may refer to [15] for more details.

2.1. **L-functions and the explicit formulas.** Let k be a function field with field of constant $\mathbb{F}_q$ and $\mathbb{K}/k$ be a Galois extension with an isomorphism $\phi_{\mathbb{K}} : \mathrm{Gal}(\mathbb{K}/k) \to G$ where G is a finite abelian group. Let $\rho : G \to \mathbb{C}^*$ be a non-principal character. The L-function $L(k, \rho \circ \phi_K, s)$ for a complex variable s is given by

$$L(k, \rho \circ \phi_K, s) = \prod_{v \in \mathcal{S}_k} \left(1 - \rho \circ \phi_{\mathbb{K}}(v) \, |v|^{-s}\right)^{-1},$$

where $\mathcal{S}_k$ is the set of places of k, and for any $v \in \mathcal{S}_k$, $|v| := q^{\deg v}$, and $\rho \circ \phi_{\mathbb{K}}(v) := \rho \circ \phi_{\mathbb{K}}((v, \mathbb{K}/k))$ where $(v, \mathbb{K}/k)$ is the Artin symbol when v is unramified in $\rho \circ \phi_{\mathbb{K}}$; if v is ramified in $\rho \circ \phi_{\mathbb{K}}$, we simply define $\rho \circ \phi_{\mathbb{K}}(v) := 0$. It is known from the Riemann hypothesis for curves that $L(k, \rho \circ \phi_{\mathbb{K}}, s)$ is polynomial of finite degree $m_{\rho,\mathbb{K}}$ in q^{-s} with constant term 1, so we can write

$$L(k, \rho \circ \phi_{\mathbb{K}}, s) = \prod_{i=1}^{m_{\rho,\mathbb{K}}} \left(1 - \sqrt{q} e(\theta_{\rho,\mathbb{K},i}) q^{-s}\right).$$

The degree $m_{\rho,\mathbb{K}}$ is given by the formula ([15])

$$m_{\rho,\mathbb{K}} = 2g_k - 2 + \deg_k \mathcal{F}(\rho \circ \phi_{\mathbb{K}}),$$

where g_k is the genus of the field k and $\mathcal{F}(\rho \circ \phi_{\mathbb{K}})$ is the Artin conductor of $\rho \circ \phi_{\mathbb{K}}$. From this we see that

$$m_{\rho,\mathbb{K}} \asymp d \quad \text{as } d = \deg_k \operatorname{Cond}(\mathbb{K}) \to \infty.$$

Taking logarithmic derivative of $L(k, \rho\circ\phi_{\mathbb{K}}, s)$ with respect to s by using the two different expressions and equating the coefficients, we obtain the the so-called "explicit formulas"

$$\sum_{i=1}^{m_{\rho,\mathbb{K}}} e(n\theta_{\rho,\mathbb{K},i}) = -q^{-|n|/2} \sum_{\substack{v\in\mathcal{S}_k \\ \deg v|n}} (\deg v)\rho \circ \phi_{\mathbb{K}}(v)^{n/\deg v}, \ \forall\, 0 \neq n \in \mathbb{Z}. \tag{3}$$

2.2. **Beurling-Selberg functions.** Let $\mathbf{I} = [-\beta/2, \beta/2]$ be an interval, symmetric about the origin, of length $0 < \beta < 1$, and $K \geq 1$ an integer. The Beurling-Selberg polynomials $I_K^{\pm}$ are trigonometric polynomials approximating the indicator function $\mathbf{1}_{\mathbf{I}}$ satisfying (see the exposition in [12, Chapter 1.2]):

- $I_K^{\pm}$ are trigonometric polynomials of degree $\leq K$.
- Monotonicity: $I_K^- \leq \mathbf{1}_{\mathbf{I}} \leq I_K^+$.
- The integral of $I_K^{\pm}$ is close to the length of the interval:

$$\int_0^1 I_K^{\pm}(x)\,\mathrm{d}x = \int_0^1 \mathbf{1}_{\mathbf{I}}(x)\,\mathrm{d}x \pm \frac{1}{K+1} \tag{4}$$

- $I_K^{\pm}(x)$ are even (since the interval $\mathbf{I}$ is symmetric about the origin).

As a consequence of (4), the non-zero Fourier coefficients of $I_K^{\pm}(x)$ satisfy

$$\left|\widehat{I}_K^{\pm}(k) - \widehat{\mathbf{1}}_{\mathbf{I}}(k)\right| \leq \frac{1}{K+1}$$

and in particular

$$\left|\widehat{I}_K^{\pm}(k)\right| \leq \frac{1}{K+1} + \min\left(\beta, \frac{\pi}{|k|}\right), \quad 0 < |k| \leq K.$$

This implies

$$\left|\widehat{I}_K^{\pm}(k)k\right| \ll 1, \quad k \in \mathbb{Z}.$$

- If $K\beta > 1$, then ([8, Propsition 4.1])

$$\sum_{n \geq 1} \widehat{I}_K^{\pm}(2n) = O(1),$$

$$\sum_{n \geq 1} n\widehat{I}_K^{\pm}(n)^2 = \frac{1}{2\pi^2} \log K\beta + O(1). \tag{5}$$

All the implied constants above are independent of K and β. We consider

$$\sum_{v \in \mathcal{S}_k} \widehat{I}_K^{\pm}(\deg v)^2 (\deg v)^2 |v|^{-1}.$$

The prime number theorem $\#\left\{v \in \mathcal{S}_k : \deg v = n\right\} = q^n/n + O\left(q^{n/2}\right)$ gives

$$\sum_{v \in \mathcal{S}_k} \widehat{I}_K^{\pm}(\deg v)^2 (\deg v)^2 |v|^{-1} \quad = \quad \sum_{1 \leq n \leq K} \widehat{I}_K^{\pm}(n)^2 \left(n + O\left(nq^{-n/2}\right)\right).$$

Using (5) we obtain (similar to Equation (7.4) in [8])

$$\sum_{v\in\mathcal{S}_k}\widehat{I}^{\pm}_{K}(\deg v)^2(\deg v)^2|v|^{-1}=\frac{1}{2\pi^2}\log K\beta+O(1)\,.$$

3. Abelian extensions with a fixed Galois group: part I

Notation. Let k be a function field with field of constant $\mathbb{F}_q$ and G be a finite abelian group of order κ, given explicitly by $G=\prod_{i=1}^{t}\mathbb{Z}/n_i\mathbb{Z}$, $n_{i+1}\mid n_i$, hence $\exp(G)=n_1$. We assume that $q\equiv 1 \pmod{n_1}$. For all positive integers n such that $\gcd(n,q)=1$, we choose compatible systems of primitive n-th roots of unity $\{\xi_n\}\subset\bar{k}\hookrightarrow\bar{k}_v$ and $\{\zeta_n\}\subset\bar{\mathbb{Q}}$ such that if $n'\mid n$, then $\xi_{n'}=\xi_n^{n/n'}$ and $\zeta_{n'}=\zeta_n^{n/n'}$. Let ι be the map such that $\iota(\xi_n)=\zeta_n$, $\gcd(n,q)=1$.

$$\begin{tikzcd}
 & \bar{k} \arrow[r, dash] & \bar{k}_v & \{\xi_n\} \arrow[r, "\iota"] & \{\zeta_n\} & \bar{\mathbb{Q}} \arrow[d, dash] \\
\mathbb{F}_q \arrow[r, dash] & k \arrow[r, dash] \arrow[u, dash] & k_v \arrow[u, dash] & & & \mathbb{Q}
\end{tikzcd}$$

Define

$$\widetilde{E}_G(k,d):=\bigcup_{H\text{ subgroup of }G}E_H(k,d),$$

or more precisely

$$\widetilde{E}_G(k,d):=\left\{\mathbb{K}:\mathrm{Gal}(\mathbb{K}/k)\xrightarrow{\phi_{\mathbb{K}}}G\ \text{ injective},\deg_k\mathrm{Cond}(\mathbb{K})=d\right\}. \tag{6}$$

The purpose of this section is to prove asymptotic formulas on $\widetilde{E}_G(k,d)$ which will be used later.

Theorem 3. *For any characters $\rho_1,\ldots,\rho_r\in\widehat{G}$ of order say $\tau_1,\ldots,\tau_r$ respectively, any distinct places $v_1,\ldots,v_r\in\mathcal{S}_k$ and any integers $\lambda_1,\ldots,\lambda_r$, define $\underline{\rho}=$*

$(\rho_1,\dots,\rho_r), \underline{v}=(v_1,\dots,v_r), \lambda=(\lambda_1,\dots,\lambda_r)$ and consider the sum

$$A_G(\underline{\rho},\underline{v},\underline{\lambda};d) := \sum_{\mathbb{K}\in \widetilde{E}_G(k,d)} \prod_{i=1}^{r} \rho_i\circ\phi_{\mathbb{K}}\left(v_i\right)^{\lambda_i}. \tag{7}$$

There is a constant $C=C(G,k)$ depending only on G and k such that

(i). *if $\tau_i\nmid\lambda_i$ for some i, then*

$$A_G(\underline{\rho},\underline{v},\underline{\lambda};d) \ll_{G,k,\eta} C^r q^{(1+\eta)d/2};$$

(ii). *if $\tau_i\mid\lambda_i$ for any $1\le i\le r$, then*

$$A_G(\underline{\rho},\underline{v},\underline{\lambda};d) = H\cdot H_{\Sigma_0} c_k^{\kappa-1} d^{\kappa-2} q^{d+\kappa-1}\left\{1+O_{G,k}\left(C^r d^{-1}\right)\right\}.$$

Here H is an absolute constant given by

$$H=\prod_{v\in\mathcal{S}_k}\left(1+(\kappa-1)|v|^{-1}\right)\left(1-|v|^{-1}\right)^{\kappa-1},$$

and the constant H_{Σ_0} is given by

$$H_{\Sigma_0}=\prod_{i=1}^{r}\frac{1+(\#\ker\rho_i-1)|v_i|^{-1}}{1+(\kappa-1)|v_i|^{-1}}.$$

The constant c_k depends only on k and can be given explicitly

$$c_k=(q-1)^{-1}q^{-g_k}h_k,$$

where h_k is the class number of k and g_k is the genus of k.

To prove Theorem 3, we use class field theory together with techniques borrowed from [19, 20]. Actually for (ii) of Theorem 3, the quantity $A_G(\underline{\rho},\underline{v},\underline{\lambda};d)$ counts the number of abelian extensions $\mathbb{K}\in\widetilde{E}_G(k,d)$ such that v_i is unramified in $\rho_i\circ\phi_{\mathbb{K}}$ for each i. In particular if $r=0$, then (ii) of Theorem 3 implies that

$$\#\widetilde{E}_G(k,d)=H\cdot\binom{d+\kappa-2}{\kappa-2}c_k^{\kappa-1}q^{d+\kappa-1}\left\{1+O_{G,k}\left(C^r d^{-1}\right)\right\}. \tag{8}$$

This is the function field analogue of results in [19, 20] with explicit error terms. It is conceivable that the class field theory and techniques from [19, 20] can be adapted to the function field setting to obtain asymptotic formulas on $A_G(\underline{\rho},\underline{v},\underline{\lambda};d)$ without much difficulty. However, the main issue here is to obtain error terms strong enough for applications in mind. As is already clear in [19, 20], and as we shall see, this is not easy. We are actually quite lucky to get a power saving as in (i) of Theorem 3. If, for example, the function fields were ordered by discriminants (i.e., the set $\widetilde{E}_G(k,d)$ consists of such $\mathbb{K}$'s with $\deg_k\operatorname{disc}(\mathbb{K})=d$), asymptotic formulas for $A_G(\underline{\rho},\underline{v},\underline{\lambda};d)$ can still be obtained, however, the error terms were too weak to be of any use for the purpose of applications. We might try to tackle this problem in the future.

Now we start the proof of Theorem 3. We follow colsely the arguments in [19]. For information on class field theory, interested readers may refer to the paper [20] for a practical overview and the book [14] for a comprehensive treatment of the theory.

3.1. **Preparation.** By class field theory, abelian extensions $\mathbb{K}\in\widetilde{E}_G(k,d)$ corresponds one-to-one to homomorphisms $\chi: J/k^*\to G$ with $\operatorname{Cond}(\chi)=\operatorname{Cond}(\mathbb{K})$ where J is the group of idèles of k and J/k^* is the idèle class group. Here k^* is understood to be its embedding image in J. For simplicity let us define

$$C(\chi):=|\operatorname{Cond}(\chi)|=q^{\deg_k\operatorname{Cond}(\mathbb{K})}.$$

For each place v of k, let k_v,o_v be the local field and the local ring at v respectively. Denote by o_v^* the group of units in o_v. We shall identify k_v^* and o_v^* with their images in J. Let $\pi_v \in o_v$ be a generator of the unique maximal ideal of o_v, then π_v can also be regarded as an element in $k_v^* \subset J$. For $\chi : J/k^* \to G$, let $\chi_v : k_v^* k^*/k^* \to G$ be the v-th component of χ. Since $q \equiv 1 \pmod{n_1}$, if v is ramified then $(1+\pi_v o_v)k^*/k^* \subset \ker(\chi_v)$. Define

$$c(\chi_v) := \begin{cases} 1 & : \quad v \text{ is ramified;} \\ 0 & : \quad v \text{ is unramified.} \end{cases}$$

Then we have

$$C(\chi) = \prod_{v \in \mathcal{S}_k} Nv^{c(\chi_v)},$$

where $Nv := |v| = q^{\deg_k v}$ is the absolute norm of v. With this preparation and by class field theory we can rewrite $A_G(\underline{\rho}, \underline{v}, \underline{\lambda}; d)$ in (7) as

$$A_G(\underline{\rho}, \underline{v}, \underline{\lambda}; d) = \sum_{\substack{\chi: J/k^* \to G \\ v_i \text{ unramified in } \rho_i \circ \chi \, \forall \, i \\ C(\chi) = q^d}} \prod_{i=1}^{r} \rho_i \circ \chi(\pi_{v_i})^{\lambda_i}.$$

Let

$$\Sigma_0 := \{v_1, \ldots, v_r\},$$

and we choose a finite subset $\Sigma' \subset \mathcal{S}_k$ of order say c such that $o_{\Sigma'}$, the ring of Σ'-integers of k, has class number 1. Define

$$\Sigma = \Sigma_0 \bigcup \Sigma', \quad r' = \#\Sigma \le r + c.$$

Then the class number of o_Σ is also 1, and the natural map $J_\Sigma/o_\Sigma^* \to J/k^*$ is an isomorphism (see [19, Lemma 2.8]), here J_Σ is the group of idèles which have components in o_v^* for all places $v \notin \Sigma$, and o_Σ^* is the group of units in o_Σ. Hence we have

$$A_G(\underline{\rho}, \underline{v}, \underline{\lambda}; d) = \sum_{\substack{\chi : J_\Sigma / o_\Sigma^* \to G \\ v_i \text{ unramified in } \rho_i \circ \chi \, \forall \, i \\ C(\chi) = q^d}} \prod_{i=1}^{r} \rho_i \circ \chi(\pi_{v_i})^{\lambda_i}.$$

Let $\mathcal{A} = \prod_{i=1}^t o_\Sigma^* / o_\Sigma^{*n_i}$. Given a $\chi : J_\Sigma \to G$ with projection $\chi_i : J_\Sigma \to \mathbb{Z}/n_i\mathbb{Z}$ (or the same from k_v^* or o_v^*), and an $\underline{\epsilon} = (\epsilon_1, \ldots, \epsilon_k) \in \mathcal{A}$, we define $\dot{\chi}(\underline{\epsilon}) = \prod_{i=1}^t \zeta_{n_i}^{\chi_i(\epsilon_i)}$, where we evaluate $\chi_i(\epsilon_i)$ using the natural map $o_\Sigma^* \to J_\Sigma$ (or to k_v^* or o_v^*). We define the twists

$$A_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; d) = \sum_{\substack{\chi : J_\Sigma \to G \\ v_i \text{ unramified in } \rho_i \circ \chi \, \forall \, i \\ C(\chi) = q^d}} \left\{ \prod_{i=1}^{r} \rho_i \circ \chi(\pi_{v_i})^{\lambda_i} \right\} \cdot \dot{\chi}(\underline{\epsilon}). \tag{9}$$

It is known from [19, Corollary 2.9] that

$$A_G(\underline{\rho}, \underline{v}, \underline{\lambda}; d) = \frac{1}{\#\mathcal{A}} \sum_{\underline{\epsilon} \in \mathcal{A}} A_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; d). \tag{10}$$

Thus to find the asymptotic behavior of $A_G(\underline{\rho}, \underline{v}, \underline{\lambda}; d)$ as $d \to \infty$, it suffices to study $A_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; d)$ for each $\underline{\epsilon}$. A standard technique is to analyze the generating function

$$F_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; s) := \sum_{\substack{\chi : J_\Sigma \to G \\ v_i \text{ unramified in } \rho_i \circ \chi \, \forall \, i}} \frac{\prod_{i=1}^r \rho_i \circ \chi(\pi_{v_i})^{\lambda_i}}{C(\chi)^s} \cdot \dot{\chi}(\underline{\epsilon}),$$

here s is a complex variable. The functions $F_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; s)$ are convenient to work with because they have Euler products ([19, 20])

$$\begin{aligned} F_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; s) &= \prod_{v \notin \Sigma} \left(\sum_{\chi_v : o_v^* \to G} \frac{\dot{\chi}_v(\underline{\epsilon})}{Nv^{c(\chi_v)s}} \right) \prod_{v \in \Sigma \setminus \Sigma_0} \left(\sum_{\chi_v : k_v^* \to G} \frac{\dot{\chi}_v(\underline{\epsilon})}{Nv^{c(\chi_v)s}} \right) \times \\ & \prod_{i=1}^{r} \left(\sum_{\substack{\chi_{v_i} : k_{v_i}^* \to G \\ v_i \text{ unramified in } \rho_i \circ \chi_{v_i}}} \frac{\rho_i \circ \chi_{v_i}(\pi_{v_i})^{\lambda_i} \dot{\chi}_{v_i}(\underline{\epsilon})}{Nv_i^{c(\chi_{v_i})s}} \right). \end{aligned}$$

3.2. **Analysis of the Euler products.** To study analytic behavior of $F_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; s)$ for the complex variable s, we need to analyze the Euler factor at each place v, in particular the values $\dot{\chi}_v(\underline{\epsilon})$. For the number field case, this was done by [19, Lemmas 2.15 and 2.16], which were motivated by the work of Taylor ([16]). The function field analogues of the two lemmas follow literally the same lines of argument, so we only record the results here.

For each place v, we choose a generator y_v of the tame inertia group of k_v (which is isomorphic to $(o_v/v)^*$) such that $y_v \equiv \xi_{Nv-1} \pmod{v}$, where ξ_{Nv-1} is the primitive $(Nv-1)$-th root of unity in $\bar{k} \subset \bar{k}_v$ which we have fixed at the beginning of this section. Then similar to [19, Lemma 2.15] we have

$$\xi_{Nv-1} = \frac{\mathrm{Frob}_v \left(y_v^{1/(Nv-1)} \right)}{y_v^{1/(Nv-1)}},$$

where the Frobenius is in the Galois group of the maximal unramified extension of k_v. [19, Lemma 2.16] also applies in the function field setting, using our choice of the compatible systems of roots of unity $\{\xi_n\}$ and $\{\zeta_n\}$. The results become much easier because $q \equiv 1 \pmod{n_1}$, hence $\xi_{n_1} \in k$. We record the values $\dot{\chi}_v(\underline{\epsilon})$ as the following.

Lemma 1. *For each place $v \notin \Sigma_0$, let $\chi_v(y_v) = g \in G$. Suppose the projections of g to $\mathbb{Z}/n_i\mathbb{Z}$ are $n_i k_i/l_i \in \mathbb{Z}/n_i\mathbb{Z}$ where $l_i \mid n_i$ and $\gcd(k_i, l_i) = 1$. Let $\underline{\epsilon}^g$ be the notation for $\prod_{i=1}^t \epsilon_i^{k_i/l_i}$. Then*

$$\dot{\chi}_v(\underline{\epsilon}) = \iota\left(\prod_{i=1}^{t} \frac{\mathrm{Frob}_v\left(\epsilon_i^{k_i/l_i}\right)}{\epsilon_i^{k_i/l_i}}\right) = \iota\left(\frac{\mathrm{Frob}_v\left(\underline{\epsilon}^g\right)}{\underline{\epsilon}^g}\right),$$

where the Frobenius is in the Galois group of the maximal extension of k unramified outside Σ_0.

We observe

Lemma 2. *For each $v \notin \Sigma_0$,*

$$\sum_{\chi_v : o_v^* \to G} \dot{\chi}_v(\underline{\epsilon}) = \begin{cases} \kappa & : \ \underline{\epsilon} = \underline{1}; \\ 0 & : \ \underline{\epsilon} \neq \underline{1}. \end{cases}$$

Proof. Let A be the sum on the left. Since $q \equiv 1 \pmod{n_1}$ and $o_v^* \simeq (o_v/v)^* \times (1 + \pi_v o_v)$, the homomorphism $\chi_v : o_v^* \to G$ factors through $(o_v/v)^*$ and hence is completely determined by its value at the generator y_v, in other words, χ_v is determined by $g \in G$ such that $\chi_v(y_v) = g$. From Lemma 1 we have

$$A = \sum_{g \in G} \iota\left(\frac{\mathrm{Frob}_v\left(\underline{\epsilon}^g\right)}{\underline{\epsilon}^g}\right).$$

If $\underline{\epsilon} = \underline{1}$, then clearly $A = \#G = \kappa$. Suppose $\underline{\epsilon} \neq \underline{1}$, then from the definition, there is a $g_0 \in G$ such that $\underline{\epsilon}^{g_0} \notin k$, hence $\frac{\mathrm{Frob}_v(\underline{\epsilon}^{g_0})}{\underline{\epsilon}^{g_0}} \neq 1$. So we have

$$\iota\left(\frac{\mathrm{Frob}_v\,(\underline{\epsilon}^{g_0})}{\underline{\epsilon}^{g_0}}\right) \cdot A = \sum_{g \in G} \iota\left(\frac{\mathrm{Frob}_v\,(\underline{\epsilon}^{g+g_0})}{\underline{\epsilon}^{g+g_0}}\right) = A,$$

from which we derive that $A = 0$. □

From Lemma 2 we find that for any $v \notin \Sigma$,

$$\sum_{\chi_v : o_v^* \to G} \frac{\dot{\chi}_v(\underline{\epsilon})}{Nv^{c(\chi_v)s}} = \begin{cases} 1 + (\kappa - 1)|v|^{-s} & : \ \underline{\epsilon} = \underline{1}; \\ 1 - |v|^{-s} & : \ \underline{\epsilon} \neq \underline{1}. \end{cases} \tag{11}$$

As for the Euler factor at $v \in \Sigma \setminus \Sigma_0$, using the isomorphism $k_v^* \simeq \langle \pi_v \rangle \times (o_v/v)^* \times (1 + \pi_v o_v)$ and $q \equiv 1 \pmod{n_1}$, a homomorphism $\chi_v : k_v^* \to G$ is determined by the values $\chi_v(\pi_v)$ and $\chi_v(y_v)$. So

$$\sum_{\chi_v : k_v^* \to G} \frac{\dot{\chi}_v(\underline{\epsilon})}{Nv^{c(\chi_v)s}} = \sum_{\mu_v : \langle \pi_v \rangle \to G} \dot{\mu}_v(\underline{\epsilon}) \sum_{\gamma_v : o_v^* \to G} \frac{\dot{\gamma}_v(\underline{\epsilon})}{Nv^{c(\gamma_v)s}}.$$

The second sum on the right over γ_v can be evaluated by (11). As for the sum over μ_v, by definition we find that

$$\sum_{\mu_v : \langle \pi_v \rangle \to G} \dot{\mu}_v(\underline{\epsilon}) = \prod_{i=1}^{t} \sum_{\mu_{v,i} : \langle \pi_v \rangle \to \mathbb{Z}/n_i\mathbb{Z}} \zeta_{n_i}^{\mathrm{ord}_v(\epsilon_i)\mu_{v,i}(\pi_v)} = \kappa \cdot \mathbf{1}_{n_i | \mathrm{ord}_v(\epsilon_i)\,\forall i},$$

here $\mathbf{1}_{n_i | \mathrm{ord}_v(\epsilon_i)\,\forall i} = 1$ if indeed $n_i \mid \mathrm{ord}_v(\epsilon_i)\, \forall 1 \leq i \leq t$; otherwise, the value is zero.

Finally for the Euler factor at $v_i \in \Sigma_0$, $1 \leq i \leq r$, which we denote by $A_{v_i}(s)$, the place v_i is unramified in $\rho_i \circ \chi_{v_i}$ if and only if $o_{v_i}^* \subset \ker \rho_i \circ \chi_{v_i}$. Writing $\chi_{v_i} = (\mu_i, \gamma_i)$ where $\mu_i : \langle \pi_{v_i} \rangle \to G$ and $\gamma_i : (o_v/v)^* \to G$, we find

$$A_{v_i}(s) = \sum_{\mu_i : \langle \pi_{v_i} \rangle \to G} \rho_i \circ \mu_i(\pi_{v_i})^{\lambda_i} \dot{\mu}_i(\underline{\epsilon}) \sum_{\gamma_i : (o_{v_i}/v_i)^* \to \ker \rho_i} \frac{\dot{\gamma}_i(\underline{\epsilon})}{Nv_i^{c(\gamma_i)s}}. \tag{12}$$

If $\underline{\epsilon} = \underline{1}$, then

$$\sum_{\mu_i : \langle \pi_{v_i} \rangle \to G} \rho_i \circ \mu_i(\pi_{v_i})^{\lambda_i} = \begin{cases} \kappa & : \quad \tau_i \mid \lambda_i, \\ 0 & : \quad \tau_i \nmid \lambda_i, \end{cases}$$

where τ_i is the order of ρ_i, and the second sum on the right of (12) is

$$\sum_{\gamma_i : (o_{v_i}/v_i)^* \to \ker \rho_i} \frac{1}{N v_i^{c(\gamma_i)s}} = 1 + \frac{\# \ker \rho_i - 1}{|v_i|^s}.$$

If $\underline{\epsilon} \neq \underline{1}$, we are contented with the fact that

$$|A_{v_i}(s)| \leq \kappa \left(1 + \frac{\# \ker \rho_i - 1}{|v_i|^{\Re s}} \right).$$

Now we summarize the above analysis on $F_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; s)$ as follows.

Lemma 3. *If $\underline{\epsilon} = \underline{1}$, and*

(1.1). *if $\tau_i \mid \lambda_i$ for any $1 \leq i \leq r$, then*

$$F_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{1}; s) = \kappa^{r'} \prod_{v \notin \Sigma_0} \left(1 + \frac{\kappa - 1}{|v|^s} \right) \prod_{i=1}^{r} \left(1 + \frac{\# \ker \rho_i - 1}{|v_i|^s} \right);$$

(1.2). *if $\tau_i \nmid \lambda_i$ for some i, then*

$$F_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{1}; s) = 0.$$

If $\underline{\epsilon} \neq \underline{1}$, then

$$F_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; s) = h(s) \prod_{v \notin \Sigma_0} \left(1 - \frac{1}{|v|^s} \right),$$

where

$$|h(s)| \leq \kappa^{r'} \prod_{i=1}^{r} \left(1 + \frac{\# \ker \rho_i - 1}{|v_i|^{\Re s}} \right).$$

3.3. **Two lemmas.** We now use Lemma 3 along with the function field version of the Tauberian Theorem ([15, Chap 17]) to prove two estimates on $A_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; d)$ defined in (9).

Lemma 4. *If $\underline{\epsilon} \neq \underline{1}$, then*

$$A_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; d) \ll_{G,k,\eta} C^r q^{(1+\eta)d/2},$$

where $C = C(G, k) > 0$ is a constant depending only on G and k.

Proof. For $\underline{\epsilon} \neq \underline{1}$, from Lemma 3 we can write

$$F_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; s) = \zeta_k(s)^{-1} H(s), \tag{13}$$

where $\zeta_k(s)$ is the zeta function of k defined by

$$\zeta_k(s) = \prod_{v \in \mathcal{S}_k} \left(1 - \frac{1}{|v|^s}\right)^{-1},$$

and the function $H(s)$ satisfies

$$|H(s)| \leq \kappa^{r'} \prod_{i=1}^{r} \left(1 + O(\kappa |v_i|^{-\Re s})\right).$$

Here $r' = \#\Sigma \leq r + c$ where $c = \#\Sigma'$ which depends only on k. This shows that $F_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; s)$ is analytic for all $s \in \mathbb{C}$ except possible poles at $\Re s = \frac{1}{2}$. This analytic statement is equivalent to Lemma 4 by using the standard Tauberian argument. For the function field version, it is most convenient to work on the variable $T = q^{-s}$. With no ambiguity we shall write the functions in T as $\zeta_k(T), H(T)$ and

$F_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; T)$. It is known that $\zeta_k(T)$ is of the form

$$\zeta_k(T) = \frac{\prod_{i=1}^{2g} \left(1 - \sqrt{q}e(\theta_i)T\right)}{(1-T)(1-qT)}, \tag{14}$$

where g is the genus of k and θ_i's are some real numbers. As for $H(T)$ we have

$$|H(T)| \leq \kappa^{r'} \prod_{i=1}^{r} \left(1 + O(\kappa |T|^{\deg v_i})\right). \tag{15}$$

We may expand

$$F_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; T) = \sum_{d=0}^{\infty} T^d A_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; d).$$

Since $F_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; T)$ is analytic for T in the region $0 < |T| < \tau = q^{-(1+\eta)/2}$, we find

$$A_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; d) = \frac{1}{2\pi i} \oint_{|T|=\tau} \frac{F_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; T)}{T^{d+1}} \, \mathrm{d}T,$$

where $\eta > 0$ is an arbitrarily small real number. Now Lemma 4 is immediate by estimating this integral, using (13) together with (14) and (15). □

Lemma 5. *If $\tau_i \mid \lambda_i$ for each $1 \leq i \leq r$, then*

$$A_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{1}; d) = \kappa^{r'} H \cdot H_{\Sigma_0} c_k^{\kappa-1} d^{\kappa-2} q^{d+\kappa-1} \left\{1 + O_{G,k}\left(C^r d^{-1}\right)\right\},$$

where the constants H, H_{Σ_0}, c_k, C are the same as in Theorem 3.

Proof. From Lemma 3 we have

$$f(s) := F_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{1}; s) = \kappa^{r'} \zeta_k(s)^{\kappa-1} \widetilde{H}(s),$$

where

$$(16)\quad \widetilde{H}(s)=\left\{\prod_{v\in\mathcal{S}_k}\left(1+\frac{\kappa-1}{|v|^s}\right)\left(1-\frac{1}{|v|^s}\right)^{\kappa-1}\right\}\left\{\prod_{i=1}^{r}\frac{\left(1+\frac{\#\ker\rho_i-1}{|v_i|^s}\right)}{\left(1+\frac{\kappa-1}{|v_i|^s}\right)}\right\}.$$

It is convenient to use $T=q^{-s}$ and we write the new functions on T as $f,\zeta_k,\widetilde{H}$ as well. Now $f(T)$ has a pole at $T=q^{-1}$ of order $\kappa-1$, coming from $\zeta_k(T)^{\kappa-1}$, and $\widetilde{H}(T)$ is analytic for T in the region $0<|T|<\tau=q^{-(1+\eta)/2}$ for an arbitrarily small real number $0<\eta<1$. We have

$$\frac{1}{2\pi i}\oint_{|T|=\tau}\frac{f(T)}{T^{d+1}}\,\mathrm{d}T=\mathrm{Res}_{T=q^{-1}}\left(\frac{f(T)}{T^{d+1}}\right)+\mathrm{Res}_{T=0}\left(\frac{f(T)}{T^{d+1}}\right).$$

From the expression for $\zeta_k(T)$ in (14) and $\widetilde{H}(s)$ in (16), we find easily that

$$\frac{1}{2\pi i}\oint_{|T|=\tau}\frac{f(T)}{T^{d+1}}\,\mathrm{d}T\ll_{G,k}C^r q^{(1+\eta)d/2}.$$

On the other hand, expanding $f(T)$ as power series in T we have

$$A_G(\underline{\rho},\underline{v},\underline{\lambda},\underline{1};d)=\mathrm{Res}_{T=0}\left(\frac{f(T)}{T^{d+1}}\right).$$

Hence to find the asymptotics for $A_G(\underline{\rho},\underline{v},\underline{\lambda},\underline{1};d)$, it suffices to compute the residue of $f(T)/T^{d+1}$ at $T=q^{-1}$, which we denote by B. The computation is straightforward: we use the formula

$$B=\frac{1}{(\kappa-2)!}\lim_{T\to q^{-1}}\left((T-q^{-1})^{\kappa-1}\frac{f(T)}{T^{d+1}}\right)^{(\kappa-2)},$$

where the exponent $(\kappa-2)$ means to take the $(\kappa-2)$-th derivative with respect to T. Since $f(T)=\kappa^{r'}\zeta_k(T)^{\kappa-1}\widetilde{H}(T)$, expanding the derivative we obtain

$$\begin{aligned} B &= \frac{\kappa^{r'}}{(\kappa-2)!}\sum_{\substack{u,v,w\geq 0\\ u+v+w=\kappa-2}}\binom{\kappa-2}{u,v,w}(-1)^u(d+1)\cdots(d+u)q^{d+1+u}\times \\ & \qquad \lim_{T\to q^{-1}}\widetilde{H}(T)^{(v)}\lim_{T\to q^{-1}}\left\{(T-q^{-1})^{\kappa-1}\zeta_k(T)^{\kappa-1}\right\}^{(w)}. \end{aligned}$$

The term from $u=\kappa-2, v=w=0$ gives the main contribution, which is

$$\begin{aligned} B_0 &= \frac{\kappa^{r'}}{(\kappa-2)!}(-1)^{\kappa-2}(d+1)\cdots(d+\kappa-2)q^{d+\kappa-1}\widetilde{H}(q^{-1})(-c_k)^{\kappa-1} \\ &= -\kappa^{r'}H\cdot H_{\Sigma_0}c_k^{\kappa-1}d^{\kappa-2}q^{d+\kappa-1}\left(1+O_{G,k}(d^{-1})\right), \end{aligned}$$

where the constants H and H_{Σ_0} come from (16) with $s=1$ (i.e. $T=q^{-1}$), and

$$c_k=-\lim_{T\to q^{-1}}(T-q^{-1})\zeta_k(T).$$

Using the expression ([15, Theorem 5.9, page 53])

$$\zeta_k(T)=\sum_{n=0}^{2g-2}b_nT^n+\frac{h_k}{q-1}\left(\frac{q^{g_k}}{1-qT}-\frac{1}{1-T}\right)T^{2g-1},$$

where h_k is the class number of k and g_k be the genus, we find easily

$$c_k=(q-1)^{-1}q^{-g_k}\,h_k.$$

All other terms in B from $u<\kappa-1$ are bounded by

$$\ll_{G,k} C^r d^{-1}B_0.$$

Combining the above estimates completes the proof of Lemma 5. □

3.4. **Proof of (i) and (ii) in Theorem 3.** We are now ready to prove (i) and (ii) in Theorem 3. If $\tau_i \nmid \lambda_i$ for some i, then for any $\underline{\epsilon} \neq \underline{1}$, from Lemma 4 we have

$$A_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; d) \ll_{G,k,\eta} C^r q^{(1+\eta)d/2}. \tag{17}$$

From (1.2) in Lemma 3 we also know that

$$A_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{1}; d) = 0.$$

Then from (10) we conclude that

$$A_G(\underline{\rho}, \underline{v}, \underline{\lambda}; d) \ll_{G,k,\eta} C^r q^{(1+\eta)d/2}.$$

So (i) is proved. Now suppose $\tau_i \mid \lambda_i$ for any $1 \leq i \leq r$. For $\underline{\epsilon} \neq \underline{1}$, we still have the estimate (17) as before. Hence from (10) we have

$$A_G(\underline{\rho}, \underline{v}, \underline{\lambda}; d) = \frac{A_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{1}; d)}{\#\mathcal{A}} + O_{G,k,\eta}\left(C^r q^{(1+\eta)d/2}\right).$$

The $A_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{1}; d)$ can be read off from Lemma 5. Hence to prove (ii) of Theorem 3, we need to show that $\#\mathcal{A} = \kappa^{r'}$. This is indeed the case: since $o_\Sigma^*/\mathbb{F}_q^*$ is a free group on $r'-1$ generators ([15, Proposition 14.2]) and $q \equiv 1 \pmod{n_i}, \forall i$, we have

$$o_\Sigma^*/o_\Sigma^{*n_i} \simeq \mathbb{F}_q^*/\mathbb{F}_q^{*n_i} \times (\mathbb{Z}/n_i\mathbb{Z})^{r'-1} \simeq (\mathbb{Z}/n_i\mathbb{Z})^{r'}.$$

Therefore

$$\#\mathcal{A} = \prod_{i=1}^{t} \#\left(\mathbb{Z}/n_i\mathbb{Z}\right)^{r'} = \prod_{i=1}^{t} n_i^{r'} = \kappa^{r'}.$$

Now (ii) is proved. This completes the proof of Theorem 3. □

4. Abelian extensions with a fixed Galois group: part II

Using notation from the previous section, we prove

Theorem 4. *For any non-principal characters $\rho_1, \ldots, \rho_r \in \widehat{G}$ and any distinct places $v_1, \ldots, v_r \in \mathcal{S}_k$ we have*

$$\sum_{\substack{\mathbb{K} \in \widetilde{E}_G(k,d) \\ v_i \text{ ramified in } \rho_i \circ \phi_{\mathbb{K}} \ \forall i}} 1 = H \prod_{i=1}^{r} (\kappa - \# \ker \rho_i) \, H'_{\Sigma_0} c_k^{\kappa-1} d^{\kappa-2} q^{d+\kappa-1} \left\{1 + O_{G,k}\left(C^r d^{-1}\right)\right\},$$

where the constants H, c_k, C are the same as in Theorem 3 and

$$H'_{\Sigma_0} = \prod_{i=1}^{r} |v_i|^{-1} \left(1 + (\kappa-1)|v|^{-1}\right)^{-1}.$$

Proof. Define

$$B_G(\underline{\rho}, \underline{v}; d) := \sum_{\substack{\mathbb{K} \in \widetilde{E}_G(k,d) \\ v_i \text{ ramified in } \rho_i \circ \phi_{\mathbb{K}} \ \forall i}} 1,$$

where $\underline{\rho} = (\rho_1, \ldots, \rho_r)$ and $\underline{v} = (v_1, \ldots, v_r)$. Since the idea of the proof is very similar to that of Theorem 3, we only sketch the main steps.

First by class field theory we can rewrite $B_G(\underline{\rho}, \underline{v}; d)$ as

$$B_G(\underline{\rho}, \underline{v}; d) = \sum_{\substack{\chi : J/k^* \to G \\ v_i \text{ ramified in } \rho_i \circ \phi_{\mathbb{K}} \ \forall i \\ C(\chi) = q^d}} 1.$$

Let $\Sigma_0 := \{v_1, \ldots, v_r\}$ and let $\Sigma' \subset \mathcal{S}_k$ be a finite subset order say c such that $o_{\Sigma'}$ has class number 1. Then define

$$\Sigma = \Sigma_0 \bigcup \Sigma', \quad r' = \#\Sigma \leq r + c.$$

The ring o_Σ also has class number 1, so using the isomorphism $J_\Sigma/o_\Sigma^* \to J/k^*$ we have

$$B_G(\underline{\rho}, \underline{v}; d) = \sum_{\substack{\chi : J_\Sigma/o_\Sigma^* \to G \\ v_i \text{ ramified in } \rho_i \circ \phi_{\mathbb{K}} \,\forall\, i \\ C(\chi) = q^d}} 1.$$

Following the same argument as in the proof of Theorem 3, we define the twists

$$B_G(\underline{\rho}, \underline{v}, \underline{\epsilon}; d) = \sum_{\substack{\chi : J_\Sigma \to G \\ v_i \text{ ramified in } \rho_i \circ \chi \,\forall\, i \\ C(\chi) = q^d}} \dot{\chi}(\underline{\epsilon}),$$

where $\underline{\epsilon} = (\epsilon_1, \dots, \epsilon_t) \in \mathcal{A} = \prod_{i=1}^t o_\Sigma^*/o_\Sigma^{*n_i}$, and given a $\chi : J_\Sigma \to G$ with projection $\chi_i : J_\Sigma \to \mathbb{Z}/n_i\mathbb{Z}$, we define $\dot{\chi}(\underline{\epsilon}) = \prod_{i=1}^t \zeta_{n_i}^{\chi_i(\epsilon_i)}$. We also have the relation

$$B_G(\underline{\rho}, \underline{v}; d) = \frac{1}{\#\mathcal{A}} \sum_{\underline{\epsilon} \in \mathcal{A}} B_G(\underline{\rho}, \underline{v}, \underline{\epsilon}; d). \tag{18}$$

The generating function of $B_G(\underline{\rho}, \underline{v}, \underline{\epsilon}; d)$ is

$$F_G(\underline{\rho}, \underline{v}, \underline{\epsilon}; d) = \sum_{\substack{\chi : J_\Sigma \to G \\ v_i \text{ ramified in } \rho_i \circ \chi \,\forall\, i}} \frac{\dot{\chi}(\underline{\epsilon})}{C(\chi)^s}.$$

It has the Euler products

$$\begin{aligned} F_G(\underline{\rho}, \underline{v}, \underline{\epsilon}; s) \;=\; & \prod_{v \notin \Sigma} \left(\sum_{\chi_v : o_v^* \to G} \frac{\dot{\chi}_v(\underline{\epsilon})}{Nv^{c(\chi_v)s}} \right) \prod_{v \in \Sigma \setminus \Sigma_0} \left(\sum_{\chi_v : k_v^* \to G} \frac{\dot{\chi}_v(\underline{\epsilon})}{Nv^{c(\chi_v)s}} \right) \times \\ & \prod_{i=1}^r \left(\sum_{\substack{\chi_{v_i} : k_{v_i}^* \to G \\ v_i \text{ ramified in } \rho_i \circ \chi}} \frac{\dot{\chi}_{v_i}(\underline{\epsilon})}{Nv_i^{c(\chi_{v_i})s}} \right). \end{aligned}$$

Notice that v is ramified in $\rho \circ \chi$ if and only if $\chi(y_v) \notin \ker \rho$ where y_v is a generator of the tame inertia group of k_v. Similar to the arguments in Theorem 3, we have:

Lemma 6. *If $\underline{\epsilon} = \underline{1}$, then*

$$F_G(\underline{\rho}, \underline{v}, \underline{1}; s) = \kappa^{r'} \prod_{i=1}^{r} (\kappa - \# \ker \rho_i) \prod_{v \notin \Sigma_0} \left(1 + \frac{\kappa - 1}{|v|^s}\right) \prod_{i=1}^{r} \frac{1}{|v_i|^s}.$$

If $\underline{\epsilon} \neq \underline{1}$, then

$$F_G(\underline{\rho}, \underline{v}, \underline{\lambda}, \underline{\epsilon}; s) = h(s) \prod_{v \notin \Sigma_0} \left(1 - \frac{1}{|v|^s}\right),$$

where

$$|h(s)| \leq \kappa^{r'} \prod_{i=1}^{r} \left(1 + \frac{\kappa}{|v_i|^{\Re s}}\right).$$

From Lemma 6, similar to the arguments in the proofs of Lemmas 4 and 5, we can obtain

$$B_G(\underline{\rho}, \underline{v}, \underline{\epsilon}; d) \ll_{G,k,\eta} C^r q^{(1+\eta)d/2}, \quad \forall \underline{\epsilon} \neq \underline{1},$$

and

$$B_G(\underline{\rho}, \underline{v}, \underline{1}; d) = \kappa^{r'} \prod_{i=1}^{r} (\kappa - \# \ker \rho_i)\, H \cdot H'_{\Sigma_0} c_k^{\kappa-1} d^{\kappa-2} q^{d+\kappa-1} \left\{1 + O_{G,k}\left(C^r d^{-1}\right)\right\},$$

where the constants H, c_k, C are the same as in Theorem 3, and H'_{Σ_0} is given by

$$H'_{\Sigma_0} = \prod_{i=1}^{r} |v_i|^{-1} \left(1 + \frac{\kappa - 1}{|v|}\right)^{-1}.$$

From these estimates and using the relation (18) we find that

$$B_G(\underline{\rho}, \underline{v}; d) = \prod_{i=1}^{r} (\kappa - \# \ker \rho_i)\, H \cdot \binom{d + \kappa - 2}{\kappa - 2} H'_{\Sigma_0} c_k^{\kappa-1} q^{d+\kappa-1} \left\{1 + O_{G,k}\left(C^r d^{-1}\right)\right\}.$$

This completes the proof of Theorem 4. □

From Theorems 3 and 4 we obtain immediately that

Corollary 1. *For any non-principal characters $\rho_1, \ldots, \rho_r \in \widehat{G}$ of order say $\tau_1, \ldots, \tau_r$ respectively and any distinct places $v_1, \ldots, v_r \in \mathcal{S}_k$.*

(i). *Let $\lambda_1, \ldots, \lambda_r$ be any integers such that $\tau_i \nmid \lambda_i$ for some i, then*

$$\frac{1}{\#\widetilde{E}_G(k,d)} \sum_{\mathbb{K} \in \widetilde{E}_G(k,d)} \prod_{i=1}^{r} \rho_i \circ \phi_{\mathbb{K}}(v_i)^{\lambda_i} \ll_{G,k,\eta} C^r q^{(-1+\eta)d)/2}.$$

(ii).

$$\frac{1}{\#\widetilde{E}_G(k,d)} \sum_{\substack{\mathbb{K} \in \widetilde{E}_G(k,d) \\ v_i \text{ unramified in } \rho_i \circ \phi_{\mathbb{K}} \, \forall i}} 1 = 1 + O_{G,k}\left(\sum_{i=1}^{r} |v_i|^{-1} \right).$$

(iii).

$$\frac{1}{\#\widetilde{E}_G(k,d)} \sum_{\substack{\mathbb{K} \in \widetilde{E}_G(k,d) \\ v_i \text{ ramified in } \rho_i \circ \phi_{\mathbb{K}} \, \forall i}} 1 \ll_{G,k} \prod_{i=1}^{r} |v_i|^{-1}.$$

Proof. (i) is immediate from (i) of Theorem 3 and (8). From (ii) of Theorem 3 we obtain

$$\frac{1}{\#\widetilde{E}_G(k,d)} \sum_{\substack{\mathbb{K} \in \widetilde{E}_G(k,d) \\ v_i \text{ unramified in } \rho_i \circ \phi_{\mathbb{K}} \, \forall i}} 1 = \prod_{i=1}^{r} \frac{1 + (\#\ker \rho_i - 1)|v_i|^{-1}}{1 + (\kappa - 1)|v_i|^{-1}} \left\{ 1 + O_{G,k}\left(C^r d^{-1} \right) \right\}.$$

It is easy to see that

$$\prod_{i=1}^{r} \frac{1 + (\#\ker \rho_i - 1)|v_i|^{-1}}{1 + (\kappa - 1)|v_i|^{-1}} = 1 + O_{G,k}\left(\sum_{i=1}^{r} |v_i|^{-1} \right).$$

(iii) is also obvious from Theorem 4, as

$$\frac{1}{\#\widetilde{E}_G(k,d)} \sum_{\substack{\mathbb{K} \in \widetilde{E}_G(k,d) \\ v_i \text{ ramified in } \rho_i \circ \phi_{\mathbb{K}} \, \forall i}} 1 \ll_{G,k} H'_{\Sigma_0} \ll_{G,k} \prod_{i=1}^{r} |v_i|^{-1}.$$

This completes the proof of Corollary 1. □

5. Distribution of zeta zeros for $\widetilde{E}_G(k,d)$

In this section we will study the distribution of zeta zeros for function fields $\mathbb{K}$ running over the set $\widetilde{E}_G(k,d)$ as $d \to \infty$, where

$$\widetilde{E}_G(k,d) := \left\{\mathbb{K} : \mathrm{Gal}(\mathbb{K}/k) \xrightarrow{\phi_{\mathbb{K}}} G \ \text{injective}, \deg_k \mathrm{Cond}(\mathbb{K}) = d\right\}.$$

More precisely, we will prove Theorem 2 for $\widetilde{E}_G(k,d)$ instead of the set $E_G(k,d)$. This is most convenient, because certain estimates of sums over $\widetilde{E}_G(k,d)$ are provided by Corollary 1. In the final Section distribution results on $E_G(k,d)$ will be derived from it.

The ideas of the proof are similar to those in [8, 4, 21]. In particular readers may readily recognise that Corollary 1 obtained in the previous section looks similar to [21, Theorem 2], which was applied in an essential way to prove a general result there. Here Corollary 1 plays the same role and the arguments are similar. However, it seems not easy to simplify the proof. For the sake of completeness, we shall produce a proof with enough details. We follow closely the presentation of [21, Section 3].

5.1. **Preparation.** For a symmetric interval $\mathbf{I} = [-\beta/2, \beta/2]$, $0 < \beta < 1/2$, let $I_l^{\pm}(x)$ be the two Beurling-Selberg polynomials of degree l defined in Section 2 such that $I_l^- \leq \mathbf{1_I} \leq I_l^+$. Since $d|\mathbf{I}| = d\beta \to \infty$ as $d \to \infty$, we can choose integers $l = l(d)$ in such a way that

$$\frac{d}{l} \to \infty,\ l\beta \to \infty,\ \text{ and } \frac{d}{l} \ll (\log l\beta)^{1/4} \ \text{ as } d \to \infty.$$

For any non-principal character $\rho : G \to \mathbb{C}^*$ and any $\mathbb{K} \in \widetilde{E}_G(k,d)$, let $\{\theta_{\rho,\mathbb{K},i} : 1 \leq i \leq m_{\rho,\mathbb{K}}\}$ be the set of angles of zeta zeros for the L-function $L(k, \rho \circ \phi_{\mathbb{K}}, s)$. From the monotonicity of $I_l^{\pm}$, we have

$$N_{\rho,l}^{-}(\mathbb{K}) \leq N_{\rho,\mathbf{I}}(\mathbb{K}) \leq N_{\rho,l}^{+}(\mathbb{K}),$$

where

$$N_{\rho,l}^{\pm}(\mathbb{K}) = \sum_{i=1}^{m_{\rho,\mathbb{K}}} I_l^{\pm}\left(\theta_{\rho,\mathbb{K},i}\right), \quad N_{\rho,\mathbf{I}}(\mathbb{K}) = \left\{i : \theta_{\rho,\mathbb{K},i} \in \mathbf{I}\right\}.$$

Let $I_l(x) = \sum_n c(n)e(nx) := I_l^{\pm}(x)$. We collect several properties of the Fourier coefficients $c(n)$ from Section 2 as follows:

(i) $c(n) = 0$ if $|n| > l$.
(ii) $c(0) = \beta + O\left(l^{-1}\right)$.
(iii) $|c(n)n| \ll 1$ for any $n \in \mathbb{Z}$.
(iv) $\sum_{v\in\mathcal{S}_k} c(\deg v)^2(\deg v)^2|v|^{-1} = \frac{1}{2\pi^2}\log(l\beta) + O(1)$.
(v) $\sum_n c(2n) \ll 1$.

Define $N_{\rho,l}(\mathbb{K}) := N_{\rho,l}^{\pm}(\mathbb{K})$. Then

$$N_{\rho,l}(\mathbb{K}) \quad = \quad \sum_{i=1}^{m_{\rho,\mathbb{K}}} I_l\left(\theta_{\rho,\mathbb{K},i}\right) = \sum_{n\in\mathbb{Z}} c(n) \sum_{i=1}^{m_{\rho,\mathbb{K}}} e\left(n\theta_{\rho,\mathbb{K},i}\right).$$

From the explicit formulas in (3) we obtain

$$N_{\rho,l}(\mathbb{K}) \quad = \quad c(0)m_{\rho,\mathbb{K}} - \sum_{0\neq n\in\mathbb{Z}} c(n)q^{-|n|/2} \sum_{\substack{v \\ \deg v|n}} (\deg v)\rho\circ\phi_{\mathbb{K}}(v)^{n/\deg v}.$$

Since $|c(n)n| \ll 1$, we have

$$\sum_{|n|\leq l} |c(n)|q^{-|n|/2} \ll 1\,.$$

Using the fact that $|\rho \circ \phi_{\mathbb{K}}(v)| \leq 1$, and $c(n) = c(-n) \in \mathbb{R}$, we derive

$$N_{\rho,l}(\mathbb{K}) = \beta m_{\rho,\mathbb{K}} - \sum_{1 \leq n \leq l} c(n) q^{-n/2} \sum_{\substack{v \in \mathcal{S}_k \\ \deg v | n}} (\deg v) \left\{ \rho \circ \phi_{\mathbb{K}}(v)^{\frac{n}{\deg v}} + \rho \circ \phi_{\mathbb{K}}(v)^{-\frac{n}{\deg v}} \right\} + O\left(\frac{m_{\rho,\mathbb{K}}}{l} \right) .$$

We may rewrite it as

$$N_{\rho,l}(\mathbb{K}) = \beta m_{\rho,\mathbb{K}} + S_{\rho,l}(\mathbb{K}) + O\left(\frac{m_{\rho,\mathbb{K}}}{l} \right) ,$$

where

$$S_{\rho,l}(\mathbb{K}) = - \sum_{\substack{v \in \mathcal{S}_k \\ r \geq 1}} c(r \deg v) |v|^{-r/2} (\deg v) \left\{ \rho \circ \phi_{\mathbb{K}}(v)^{r} + \rho \circ \phi_{\mathbb{K}}(v)^{-r} \right\} .$$

Now it is easy to see that

$$S_{\rho,l}(\mathbb{K}) \ll \sum_{1 \leq n \leq l} q^{-n/2} \sum_{\substack{v \in \mathcal{S}_k \\ \deg v | n}} 1 \ll \sum_{1 \leq n \leq l} q^{n/2} \ll q^{l/2},$$

and hence

$$|N_{\rho,l}(\mathbb{K}) - \beta m_{\rho,\mathbb{K}}| \ll \frac{m_{\rho,\mathbb{K}}}{l} + q^{l/2} .$$

Noting that $|\mathbf{I}| = \beta$, $m_{\rho,\mathbb{K}} \asymp d$ and taking $l \asymp \log_q d - \log_q \log d$, we have deduced that the zeros are uniformly distributed:

Proposition 5. *As $d \to \infty$, for each $\mathbb{K} \in \widetilde{E}_G(k,d)$, every fixed symmetric interval $\mathbf{I} = [-\beta/2, \beta/2]$ contains asymptotically $m_{\rho,\mathbb{K}}|\mathbf{I}|$ angles $\theta_{\rho,\mathbb{K},i}$ for each ρ. In fact*

$$N_{\rho,\mathbf{I}}(\mathbb{K}) = m_{\rho,\mathbb{K}}|\mathbf{I}| + O\left(\frac{m_{\rho,\mathbb{K}}}{\log m_{\rho,\mathbb{K}}} \right) .$$

Denote

$$T_{\rho,l}(\mathbb{K}) = -\sum_{v\in\mathcal{S}_k} c(\deg v)\deg v|v|^{-1/2}\left\{\rho\circ\phi_{\mathbb{K}}(v)+\rho\circ\phi_{\mathbb{K}}(v)^{-1}\right\}, \tag{19}$$

and

$$\triangle_{\rho,l}(\mathbb{K}) = -\sum_{v\in\mathcal{S}_k} c(2\deg v)\deg v|v|^{-1}\left\{\rho\circ\phi_{\mathbb{K}}(v)^2+\rho\circ\phi_{\mathbb{K}}(v)^{-2}\right\}. \tag{20}$$

Then

$$S_{\rho,l}(\mathbb{K}) - T_{\rho,l}(\mathbb{K}) - \triangle_{\rho,l}(\mathbb{K}) \;=\; -\sum_{\substack{v\in\mathcal{S}_k\\ r\geq 3}} c(r\deg v)|v|^{-r/2}(\deg v)\left\{\rho\circ\phi_{\mathbb{K}}(v)^r+\rho\circ\phi_{\mathbb{K}}(v)^{-r}\right\}.$$

It is easy to see that this is bounded by

$$\ll \sum_{\substack{v\in\mathcal{S}_k\\ r\geq 3}} q^{-r\deg v/2} \leq \sum_{r\geq 3}\sum_{n\leq l/3} q^{-rn/2}q^n \ll 1.$$

Therefore

$$N_{\rho,l}(\mathbb{K}) - m_{\rho,\mathbb{K}}\beta = T_{\rho,l}(\mathbb{K}) + \triangle_{\rho,l}(\mathbb{K}) + O\left(\frac{m_{\rho,\mathbb{K}}}{l}\right). \tag{21}$$

We denote by $\langle\bullet\rangle$ the mean value of any quantity defined on $\widetilde{E}_G(k,d)$, that is, let $\chi : \widetilde{E}_G(k,d)\to\mathbb{C}$ be a map, then

$$\langle\chi\rangle := \frac{1}{\#\widetilde{E}_G(k,d)}\sum_{\mathbb{K}\in\widetilde{E}_G(k,d)}\chi(\mathbb{K}).$$

The goal is to compute for any fixed nonnegative integers $r_1, r_2, \ldots, r_t$ the moment $\left\langle\prod_{j=1}^t\left(N_{\rho_j,l}(\bullet)-m_{\rho_j,\bullet}\beta\right)^{r_j}\right\rangle$. For this purpose we need to compute various moments for $\triangle_{\rho_j,l}(\bullet)$ and $T_{\rho_j,l}(\bullet)$ first. To simplify notation, in what follows the implied constants in "O" and "$\ll$" may depend on G, k and the integer $r = \sum_j r_j$.

5.2. **Moments of $\triangle_{\rho,l}(\mathbb{K})$.** For each ρ of order $\tau \geq 2$, we may consider two cases.

Case (1). $\tau \geq 3$. Then for each fixed positive integer r, we have from (20)

$$\triangle_{\rho,l}(\mathbb{K})^{2r} = \sum_{v_1,\ldots,v_{2r}\in\mathcal{S}_k} \prod_{i=1}^{2r} c(2\deg v_i)|v_i|^{-1}\deg v_i \sum_{\lambda_1,\ldots,\lambda_{2r}\in\{1,-1\}} \prod_{i=1}^{2r} \rho\circ\phi_{\mathbb{K}}(v_i)^{2\lambda_i}\,.$$

Hence

$$\langle(\triangle_{\rho,l})^{2r}\rangle = \sum_{v_1,\ldots,v_{2r}\in\mathcal{S}_k} \prod_{i=1}^{2r} c(2\deg v_i)|v_i|^{-1}\deg v_i \sum_{\lambda_1,\ldots,\lambda_{2r}\in\{1,-1\}} \left\langle \prod_{i=1}^{2r} \rho\circ\phi_{\mathbb{K}}(v_i)^{2\lambda_i} \right\rangle\,.$$

Consider $v_1^{2\lambda_1}\cdots v_{2r}^{2\lambda_{2r}}$ as an element of $\mathrm{Div}(k)$, the free abelian multiplicative group generated by all the places of k. If $v_1^{2\lambda_1}\cdots v_{2r}^{2\lambda_{2r}}$ is not a τ-th power in $\mathrm{Div}(k)$, then by (i) of Corollary 1, we have

$$\left\langle \prod_{i=1}^{2r} \rho\circ\phi_{\mathbb{K}}(v_i)^{2\lambda_i} \right\rangle \ll_\eta C^r q^{(-1+\eta)d/2}.$$

Since $d/l \to \infty$, the total contribution in this case is

$$\langle(\triangle_{\rho,l})^{2r}\rangle_1 \ll_\eta \sum_{\substack{v_1,\ldots,v_{2r}\\ \deg v_i\leq l}} \prod_{i=1}^{2r} |v_i|^{-1} \sum_{\lambda_1,\ldots,\lambda_{2r}\in\{1,-1\}} C^{2r}q^{(-1+\eta)d/2} \ll 1.$$

If $v_1^{2\lambda_1}\cdots v_{2r}^{2\lambda_{2r}}$ is a τ-th power in $\mathrm{Div}(k)$, since $\tau \geq 3$, for this to happen, each v_i must be paired off with at least one $v_j, i\neq j$, $v_i = v_j$. Hence the total contribution in this case is at most

$$\langle(\triangle_{\rho,l})^{2r}\rangle_2 \ll \left(\sum_v |v|^{-2}\right)^r \ll 1\,.$$

Case (2) $\tau = 2$. Then

$$\triangle_{\rho,l}(\mathbb{K}) = -2 \sum_{\substack{v\in\mathcal{S}_k \\ v\,\text{unramified in }\rho\circ\phi_{\mathbb{K}}}} c(2\deg v)|v|^{-1}(\deg v) = \triangle_1(\mathbb{K}) + \triangle_2(\mathbb{K}),$$

where

$$\begin{aligned} \triangle_1(\mathbb{K}) &= -2\sum_{v\in\mathcal{S}_k} c(2\deg v)|v|^{-1}(\deg v) = -2\sum_{1\le n\le l/2} c(2n)nq^{-n} \sum_{\substack{v\in\mathcal{S}_k \\ \deg v=n}} 1 \\ &= -2\sum_{1\le n\le l/2} c(2n)nq^{-n}\left(q^n/n + O(q^{n/2})\right) \\ &= -2\sum_{1\le n\le l/2} c(2n) + O(1) \ll 1, \text{ from (v)}, \end{aligned}$$

and

$$\triangle_2(\mathbb{K}) = 2 \sum_{\substack{v\in\mathcal{S}_k \\ v\,\text{ramified in }\rho\circ\phi_{\mathbb{K}}}} c(2\deg v)|v|^{-1}(\deg v).$$

Since $|c(n)n| \ll 1$ we find

$$\begin{aligned} \langle|(\triangle_2)^r|\rangle &\ll \left\langle \sum_{\substack{v_1,\dots,v_r\in\mathcal{S}_k \\ v_i\text{ ramified in }\rho\circ\phi_{\mathbb{K}}\,\forall i}} |v_1|^{-1}\cdots|v_r|^{-1} \right\rangle \\ &= \sum_{v_1,\dots,v_r\in\mathcal{S}_k} |v_1|^{-1}\cdots|v_r|^{-1}\frac{1}{\#\widetilde{E}_G(k,d)} \sum_{\substack{\mathbb{K}\in\widetilde{E}_G(k,d) \\ v_i\text{ ramified in }\rho\circ\phi_{\mathbb{K}}\,\forall i}} 1. \end{aligned}$$

Now by (iii) of Corollary 1 we obtain

$$\begin{aligned}\langle|(\triangle_2)^r|\rangle &\ll \sum_{v_1,\ldots,v_r\in\mathcal{S}_k}|v_1|^{-1}\cdots|v_r|^{-1}\prod_{v\in\{v_1,\ldots,v_r\}}|v|^{-1}\\ &\ll \left(\sum_{v\in\mathcal{S}_k}|v|^{-2}\right)^r \ll 1.\end{aligned}$$

Combining the two cases above we conclude that

$$\langle(\triangle_{\rho,l})^{2r}\rangle \ll 1\,. \tag{22}$$

5.3. **Moments of $T_{\rho,l}(\mathbb{K})$.** For each fixed positive integer r, from (19) we have

$$T_{\rho,l}(\mathbb{K})^r=(-1)^r\sum_{v_1,\ldots,v_r\in\mathcal{S}_k}\prod_{i=1}^r c(\deg v_i)|v_i|^{-1/2}(\deg v_i)\sum_{\lambda_1,\ldots,\lambda_r\in\{1,-1\}}\rho\circ\phi_{\mathbb{K}}\left(v_1^{\lambda_1}\cdots v_r^{\lambda_r}\right)\,.$$

Hence

$$\langle(T_{\rho,l})^r\rangle=(-1)^r\sum_{v_1,\ldots,v_r\in\mathcal{S}_k}\prod_{i=1}^r c(\deg v_i)|v_i|^{-1/2}(\deg v_i)\sum_{\lambda_1,\ldots,\lambda_r\in\{1,-1\}}\left\langle\rho\circ\phi_{\mathbb{K}}\left(v_1^{\lambda_1}\cdots v_r^{\lambda_r}\right)\right\rangle\,.$$

If $v_1^{\lambda_1}\cdots v_r^{\lambda_r}$ is not a τ-th power in Div(k), the total contribution in this case, from (i) of Corollary 1, is

$$\langle(T_{\rho,l})^r\rangle_1\ll\sum_{\substack{v_1,\ldots,v_r\in\mathcal{S}_k\\ \deg v_i\le l}}\prod_{i=1}^r|v_i|^{-1/2}\sum_{\lambda_1,\ldots,\lambda_r\in\{1,-1\}}C^r q^{(-1+\eta)d/2}\ll 1.$$

If $v_1^{\lambda_1}\cdots v_r^{\lambda_r}$ is a τ-th power in Div(k), for this to happen, each v_i must be paired off with another $v_j, i\neq j$, $v_i=v_j$. The most "economic" way of doing that is that each v_i is paired off with exactly one $v_j, i\neq j, v_i=v_j$, so that $r=2s$ must be even. The number of choices for such arrangement is $(2s)!/s!2^s$. Moreover, the exponents must satisfy the condition $\lambda_i+\lambda_j\equiv 0 \pmod{\tau}$, and there are exactly $2r_\rho$ choices for $\lambda_i, \lambda_j \in \{1, -1\}$, where $r_\rho = 1$ if $\tau \geq 3$, and $r_\rho = 2$ if $\tau = 2$, where τ is the order of ρ. Hence the contribution in this case is

$$\langle (T_{\rho,l})^r \rangle_0 = (2r_\rho)^s \frac{(2s)!}{s!2^s} \sum_{\substack{v_1,\ldots,v_s \in \mathcal{S}_k \\ \text{distinct}}} \prod_{i=1}^{s} c(\deg v_i)^2 |v_i|^{-1} (\deg v_i)^2 \left\langle \rho^\tau \circ \phi_{\mathbb{K}}(v_1 \cdots v_s) \right\rangle \, .$$

Since ρ has order τ, from (ii) of Corollary 1 we find that

$$\langle \rho^\tau \circ \phi_{\mathbb{K}}(v_1 \cdots v_s) \rangle = \frac{1}{\# \widetilde{E}_G(k,d)} \sum_{\substack{\mathbb{K} \in \widetilde{E}_G(k,d) \\ v_i \text{ unramified in } \rho_i \circ \phi_{\mathbb{K}} \ \forall \, i}} 1 = 1 + O\left(\sum_{i=1}^{s} |v_i|^{-1} \right).$$

The contribution from the error term $O\left(\sum_{i=1}^{s} |v_i|^{-1}\right)$ is bounded by

$$E \ll \left(\sum_{v \in \mathcal{S}_k} c(\deg v)^2 (\deg v)^2 |v|^{-1} \right)^{s-1} \left(\sum_{v \in \mathcal{S}_k} |v|^{-2} \right).$$

Using property (iv) of $c(n)$ and the estimate $\sum_{v \in \mathcal{S}_k} |v|^{-2} \ll 1$, we find

$$E \ll (\log l\beta)^{s-1} \, .$$

The main term is

$$\frac{(r_\rho)^s (2s)!}{s!} \sum_{\substack{v_1,\ldots,v_s \in \mathcal{S}_k \\ \text{distinct}}} \prod_{i=1}^{s} c(\deg v_i)^2 |v_i|^{-1} (\deg v_i)^2 \, .$$

Now we remove the restriction that $v_1, \ldots, v_s$ are distinct, introducing again an error of $O\left((\log l\beta)^{s-2}\right)$. This gives us

$$\langle (T_{\rho,l})^r \rangle_0 = \frac{(r_\rho)^s (2s)!}{s!} \left(\sum_{v \in \mathcal{S}_k} c(\deg v)^2 (\deg v)^2 |v|^{-1} \right)^s + O\left((\log l\beta)^{s-1}\right).$$

Using property (iv) of $c(n)$ again we derive that

$$\langle (T_{\rho,l})^r \rangle_0 \;=\; \frac{(r_\rho)^s(2s)!}{s!}\left(\frac{1}{2\pi^2}\log(l\beta)+O(1)\right)^s + O\left((\log l\beta)^{s-1}\right),$$

and from it we obtain

$$\langle (T_{\rho,l})^r \rangle_0 \;=\; \frac{(r_\rho)^s(2s)!}{2^s\pi^{2s}s!}\left(\log l\beta\right)^s + O\left((\log l\beta)^{s-1}\right),$$

where $r=2s$ is an even number.

On the other hand, if each v_i is paired off with another $v_j, i\neq j$, $v_i=v_j$, but it is not the most "economic", that is, there is one v_i which is paired off with at least two others $v_{j_1}, v_{j_2}, i\neq j_1\neq j_2$ with $v_i=v_{j_1}=v_{j_2}$. Similar to [21, 4.2.2 Case two], we find easily that the total contribution from this case is bounded by

$$\ll (\log l\beta)^{(r-3)/2}.$$

We conclude that

$$\langle (T_{\rho,l})^r \rangle = \frac{(r_\rho)^{r/2}\delta(r)r!}{2^{r/2}\pi^r(r/2)!}(\log l\beta)^{r/2} + O\left((\log l\beta)^{-1+r/2}\right),$$

where $\delta(r)=1$ if r is even and $\delta(r)=0$ if r is odd.

5.4. **General moments of $T_{\rho,l}$.** Let $\rho_1,\ldots,\rho_t\in\widehat{G}$ be non-principal characters of order $\tau_1,\ldots,\tau_t$ respectively. For any nonnegative integers $r_1,\ldots,r_t$, let $r=\sum_{j=1}^t r_j$. We have

$$\prod_{j=1}^t T_{\rho_j,l}(\mathbb{K})^{r_j} = (-1)^r\sum_{v_{j,i}}\prod_{j,i} c\left(\deg v_{j,i}\right)|v_{j,i}|^{-1/2}\deg v_{j,i}\sum_{\lambda_{j,i}\in\{1,-1\}}\prod_{j,i}\rho_j\circ\phi_{\mathbb{K}}\left(v_{j,i}^{\lambda_{j,i}}\right),$$

where the index j, i run over the range $1 \leq j \leq t$ and $1 \leq i \leq r_j$. Hence

$$\left\langle \prod_{j=1}^{t} \left(T_{\rho_j,l}\right)^{r_j} \right\rangle = (-1)^r \sum_{v_{j,i}} \prod_{j,i} c\left(\deg v_{j,i}\right) |v_{j,i}|^{-1/2} (\deg v_{j,i}) \sum_{\lambda_{j,i} \in \{1,-1\}} \left\langle \prod_{j,i} \rho_j \circ \phi_{\mathbb{K}} \left(v_{j,i}^{\lambda_{j,i}}\right) \right\rangle .$$

Similarly, if some $v_{j,i}$ is not paired off with another $v_{j',i'}$, then by (i) of Corollary 1, the total contribution in this case is bounded by $O(1)$; if each $v_{j,i}$ is paired off with another $v_{j',i'}$ and there is one element that is paired off with at least two other elements, using similar argument the total contribution in this case is bounded by $O\left((\log K\beta)^{(r-3)/2}\right)$. The remaining cases are that each $v_{j,i}$ is paired off with exactly one $v_{j',i'}$ where $(j,i) \neq (j',i')$. Since $\rho_i \rho_j \neq 1$ for any $i \neq j$, if there are $(j,i), (j',i')$ with $j \neq j'$ such that $v_{j,i} = v_{j',i'}$, then by (i) of Corollary 1, the total contribution again is bounded by $O(1)$. The main contribution comes from the case that for each j, $v_{j,i}$ is paired off with exactly one $v_{j,i'}$ with $i \neq i'$. For this to happen, then for each j, $r_j = 2s_j$ must be even, and the number of choices of $v_{j,i}$ and $\lambda_{j,i}$ is $(2r_{\rho_j})^{s_j} \frac{(2s_j)!}{2^{s_j}(s_j)!}$. Hence the total contribution in this case is

$$\left\langle \prod_{j=1}^{t} \left(T_{\rho,l}\right)^{r_j} \right\rangle_0 = \prod_{j=1}^{t} (2r_{\rho_j})^{s_j} \frac{(2s_j)!}{(s_j)!2^{s_j}} \sum_{\substack{v_{j,i} \in \mathcal{S}_k \\ \text{all distinct}}} \prod_{j,i} c(\deg v_{j,i})^2 |v_{j,i}|^{-1} (\deg v_{j,i})^2 \left\langle \prod_{j,i} \rho_j^{\tau_j} \circ \phi_{\mathbb{K}}\left(v_{j,i}\right) \right\rangle ,$$

where the index j, i runs over the range $1 \leq j \leq t$ and $1 \leq i \leq s_j$. Since

$$\left\langle \prod_{j,i} \rho_j^{\tau_j} \circ \phi_{\mathbb{K}}\left(v_{j,i}\right) \right\rangle = 1 + O\left(\sum_{j,i} |v_{j,i}|^{-1}\right) ,$$

the error term arising from $O\left(\sum_{j,i} |v_{j,i}|^{-1}\right)$ is $E \ll (\log K\beta)^{-1+\sum_j s_j}$, and the main term is

$$\prod_{j=1}^{t} (2r_{\rho_j})^{s_j} \frac{(2s_j)!}{(s_j)!2^{s_j}} \sum_{\substack{v_{j,i} \in \mathcal{S}_k \\ \text{all distinct}}} \prod_{j,i} c(\deg v_{j,i})^2 |v_{j,i}|^{-1} (\deg v_{j,i})^2 .$$

We may remove the restriction that all $v_{j,i}$'s are distinct, introducing again an error of $O\left((\log K\beta)^{-2+\sum_j s_j}\right)$. This gives us

$$\left\langle \prod_{j=1}^{t} \left(T_{\rho_j,l}\right)^{r_j} \right\rangle_0 = \prod_{j=1}^{t} \frac{(r_{\rho_j})^{s_j}(2s_j)!}{(s_j)!} \left(\sum_{v\in\mathcal{S}_k} c(\deg v)^2(\deg v)^2|v|^{-1}\right)^{s_j} +O\left((\log l\beta)^{-1+\sum_j s_j}\right).$$

From it we obtain

$$\left\langle \prod_{j=1}^{t} \left(T_{\rho_j,l}\right)^{r_j} \right\rangle_0 = \prod_{j=1}^{t} \frac{(r_{\rho_j})^{s_j}(2s_j)!}{2^{s_j}\pi^{2s_j}s_j!}(\log l\beta)^{s_j} + O\left((\log l\beta)^{-1+\sum_j s_j}\right).$$

Combining the above estimates together we conclude that

$$(23)\quad \left\langle \prod_{j=1}^{t} \left(T_{\rho_j,l}\right)^{r_j} \right\rangle = \prod_{j=1}^{t} \frac{(r_{\rho_j})^{r_j/2}\delta(r_j)(r_j)!}{2^{r_j/2}\pi^{r_j}(r_j/2)!}(\log l\beta)^{r_j/2} + O\left((\log l\beta)^{-1+r/2}\right),$$

where $\delta(s)=1$ if s is even and $\delta(s)=0$ if s is odd, and $r=\sum_{j=1}^{t} r_j$, and the implied constant in "O" may depend on G, k and r.

5.5. **Proof of Theorem 2 for $\widetilde{E}_G(k,d)$.** Very similar to [21, Section 5], combining the results obtained in (23), (22) and using (21) we can obtain

$$(24)\quad \left\langle \prod_{j=1}^{t} \left(\frac{N_{\rho_j,l}(\bullet)-\beta m_{\rho,\bullet}}{\sqrt{\frac{r_{\rho_j}}{\pi^2}\log(l\beta)}} \right)^{r_j} \right\rangle = \prod_{j=1}^{t} \frac{\delta(r_j)r_j!}{2^{r_j/2}(r_j/2)!} + O\left((\log l\beta)^{-1/4}\right).$$

Since $N^-_{\rho_j,l}(\mathbb{K}) \le N_{\rho_j,\mathbf{I}}(\mathbb{K}) \le N^+_{\rho_j,l}(\mathbb{K})$ for each ρ_j, we have taken for granted in [21, Section 5] that in Equation (24) the terms $N_{\rho_j,l}(\bullet)=N^{\pm}_{\rho_j,l}(\bullet)$ could be replaced by $N_{\rho_j,\mathbf{I}}(\bullet)$ and Equation (24) still holds true. Since for a standard Gaussian distribution, the odd moments vanish and the even moments are

$$\frac{1}{\sqrt{2\pi}}\int_{\infty}^{\infty} x^{2r}e^{-x^2/2}\mathrm{d}\,x = \frac{(2r)!}{2^r r!},$$

we shall conclude directly that as $\mathbb{K}$ runs through $\widetilde{E}_G(k,d)$ with $d \to \infty$,

$$\left(\frac{N_{\rho_1,\mathbf{I}}(\mathbb{K}) - m_{\rho_1,\mathbb{K}}\beta}{\sqrt{\frac{r_{\rho_1}}{\pi^2}\log m_{\rho_1,\mathbb{K}}\beta}}, \ldots, \frac{N_{\rho_t,\mathbf{I}}(\mathbb{K}) - m_{\rho_t,\mathbb{K}}\beta}{\sqrt{\frac{r_{\rho_t}}{\pi^2}\log m_{\rho_t,\mathbb{K}}\beta}} \right)$$

converges weakly to t identical independent standard Gaussian distributions.

That in Equation (24) the terms $N_{\rho_j,l}(\bullet) = N^{\pm}_{\rho_j,l}(\bullet)$ could be replaced by $N_{\rho_j,\mathbf{I}}(\bullet)$ and Equation (24) still holds true – rigorously speaking, that is correct but not quite obvious and needs to be proved. We take this opportunity to provide an argument here.

Define

$$W_{\rho,l}(\mathbb{K}) \quad := \quad N^{+}_{\rho,l}(\mathbb{K}) - N^{-}_{\rho,l}(\mathbb{K}).$$

We have from (21)

$$W_{\rho,l}(\mathbb{K}) \quad = \quad W'_{\rho,l}(\mathbb{K}) + W''_{\rho,l}(\mathbb{K}) + O\left(\frac{d}{l}\right),$$

where

$$W'_{\rho,l}(\mathbb{K}) = \sum_{v \in \mathcal{S}_k} \frac{(\deg v)\,(c^{-}(\deg v) - c^{+}(\deg v))}{|v|^{1/2}} \left\{\rho \circ \phi_{\mathbb{K}}(v) + \rho \circ \phi_{\mathbb{K}}(v)^{-1}\right\},$$

and

$$W''_{\rho,l}(\mathbb{K}) = \sum_{v \in \mathcal{S}_k} \frac{(\deg v)\,(c^{-}(2\deg v) - c^{+}(2\deg v))}{|v|} \left\{\rho \circ \phi_{\mathbb{K}}(v)^2 + \rho \circ \phi_{\mathbb{K}}(v)^{-2}\right\}.$$

Since

$$\left|c^{+}(n) - c^{-}(n)\right| \le \frac{1}{2(l+1)},$$

we find that

$$W''_{\rho,l}(\mathbb{K}) \ll \frac{1}{l} \sum_{\substack{v\in\mathcal{S}_k\\ \deg v\leq l}} (\deg v)|v|^{-1} \ll \frac{1}{l}\sum_{n\leq l} nq^{-n}\frac{q^n}{n} \ll 1.$$

Hence

$$W_{\rho,l}(\mathbb{K}) = W'_{\rho,l}(\mathbb{K}) + O\left(\frac{d}{l}\right). \tag{25}$$

Next for any non-negative integers $r_1,\dots,r_t$, let $r=\sum_j r_j$, we obtain

$$\left\langle \prod_{j=1}^{t} (W'_{\rho_j,l})^{2r_j} \right\rangle \ll l^{-2r} \sum_{\substack{v_{j,i}\in\mathcal{S}_k\\ \deg v_{j,i}\leq l}} \prod_{j,i} \frac{\deg v_{j,i}}{|v_{j,i}|^{1/2}} \sum_{\lambda_{j,i}\in\{1,-1\}} \left\langle \prod_{j,i} \rho_j\circ\phi_{\mathbb{K}}(v_{j,i})^{\lambda_{j,i}} \right\rangle,$$

where the index j,i runs over the range $1\leq j\leq t$ and $1\leq i\leq 2r_j$.

Again, if one $v_{j,i}$ is not paired off with any other $v_{j',i'}$, then by (i) of Corollary 1, the contribution for this case is bounded by $O(1)$. If for any j,i, the place $v_{j,i}$ is paired off with another $v_{j',i'}$, then the total contribution for this case is bounded by

$$\begin{aligned} &\ll\ l^{-2r}\left(\sum_{\substack{v\in\mathcal{S}_k\\ \deg v\leq l}} (\deg v)^2|v|^{-1}\right)^r = l^{-2r}\left(\sum_{1\leq n\leq l} n^2q^{-n} \sum_{\substack{v\in\mathcal{S}_k\\ \deg v=n}} 1\right)^r \\ &\ll\ l^{-2r}\left(\sum_{1\leq n\leq l} n^2q^{-n}\frac{q^n}{n}\right)^r \ll 1. \end{aligned}$$

So we have

$$\left\langle \prod_{j=1}^{t} (W'_{\rho_j,l})^{2r_j} \right\rangle \ll 1.$$

Using (25) we obtain

$$\begin{aligned}\left|\left\langle\prod_{j=1}^{t}(W_{\rho_j,l})^{r_j}\right\rangle\right| &\ll \sum_{u_j+v_j=r_j,\,\forall j}\left\langle\left|\prod_{j=1}^{t}(W'_{\rho_j,l})^{u_j}\left(\frac{d}{l}\right)^{v_j}\right|\right\rangle\\ &\ll \sum_{u_j+v_j=r_j,\,\forall j}\left(\frac{d}{l}\right)^{\sum_j v_j}\left\langle\prod_{j=1}^{t}(W'_{\rho_j,l})^{2u_j}\right\rangle^{1/2}.\end{aligned}$$

Since $d/l \ll (\log l\beta)^{1/4}$, this gives

$$\left|\left\langle\prod_{j=1}^{t}(W_{\rho_j,l})^{r_j}\right\rangle\right| \ll \sum_{u_j+v_j=r_j,\,\forall j}\left(\frac{d}{l}\right)^{\sum_j v_j} \ll (\log l\beta)^{r/4}. \tag{26}$$

With this estimate, and noting that

$$N_{\rho_j,\mathbf{I}}(\mathbb{K})-\beta m_{\rho_j,\mathbb{K}} = N^{-}_{\rho_j,l}(\mathbb{K})-\beta m_{\rho_j,\mathbb{K}}+V_{\rho_j,l}(\mathbb{K}),$$

where

$$0\le V_{\rho_j,l}(\mathbb{K}) = N_{\rho_j,\mathbf{I}}(\mathbb{K})-N^{-}_{\rho_j,l}(\mathbb{K})\le W_{\rho_j,l}(\mathbb{K}),$$

we find that

$$\prod_{j=1}^{t}\left(N_{\rho_j,\mathbf{I}}(\mathbb{K})-\beta m_{\rho_j,\mathbb{K}}\right)^{r_j} = \prod_{j=1}^{t}\left(N^{-}_{\rho_j,l}(\mathbb{K})-\beta m_{\rho_j,\mathbb{K}}\right)^{r_j}+E(\mathbb{K}),$$

where

$$|E(\mathbb{K})| \ll \sum_{\substack{u_j+v_j=r_j,\,\forall j\\ \sum_j v_j\ge 1}}\left|\prod_{j=1}^{t}\left(N^{-}_{\rho,l}(\mathbb{K})-\beta m_{\rho,\mathbb{K}}\right)^{u_j}W_{\rho_j,l}(\mathbb{K})^{v_j}\right|.$$

Using the Cauchy-Schwartz inequality, we obtain

$$\langle |E(\bullet)| \rangle \ll \sum_{\substack{u_j+v_j=r_j,\forall j\\ \sum_j v_j \geq 1}} \left\langle \prod_{j=1}^{t} \left(N^{-}_{\rho,l}(\bullet) - \beta m_{\rho,\bullet}\right)^{2u_j} \right\rangle^{1/2} \left\langle \prod_{j=1}^{t} (W_{\rho_j,l})^{2v_j} \right\rangle^{1/2}.$$

From (24) and (26) we have

$$\langle |E(\bullet)| \rangle \ll \sum_{\substack{u_j+v_j=r_j,\forall j\\ \sum_j v_j \geq 1}} (\log l\beta)^{\sum_j u_j/2} (\log l\beta)^{\sum_j v_j/4} \ll (\log l\beta)^{\frac{r}{2}-\frac{1}{4}}.$$

From the above and (24) we conclude that

$$\left\langle \prod_{j=1}^{t} \left(\frac{N_{\rho_j,\mathbf{I}}(\bullet) - \beta m_{\rho_j,\bullet}}{\sqrt{\frac{r_{\rho_j}}{\pi^2}\log(l\beta)}} \right)^{r_j} \right\rangle = \prod_{j=1}^{t} \frac{\delta(r_j)(r_j)!}{2^{r_j/2}\,(r_j/2)!} + O\left((\log l\beta)^{-1/4} \right), \tag{27}$$

where the implied constant in "O" may depend on G, k and $r = \sum_j r_j$. In the denominators we can also replace l by $m_{\rho_j,\mathbb{K}}$ because

$$\log(l\beta) \sim \log(m_{\rho_j,\mathbb{K}}\beta).$$

This concludes the proof of Theorem 2 for $\widetilde{E}_G(k,d)$ as $d \to \infty$. □

6. Proof of Theorems 1 and 2

Theorem 2 on $E_G(k,d)$ can be derived easily from the result on $\widetilde{E}_G(k,d)$. For simplicity we define

$$a_\rho(\mathbb{K}) := \frac{N_{\rho,\mathbf{I}}(\mathbb{K}) - \beta m_{\rho,\mathbb{K}}}{\sqrt{\frac{r_\rho}{\pi^2}\log(l\beta)}}.$$

Equation (27) shows that

$$\frac{1}{\#\widetilde{E}_G(k,d)} \sum_{\mathbb{K}\in\widetilde{E}_G(k,d)} \prod_{j=1}^{t} a_{\rho_j}(\mathbb{K})^{r_j} = \prod_{j=1}^{t} \frac{\delta(r_j)(r_j)!}{2^{r_j/2}\,(r_j/2)!} + O\left((\log l\beta)^{-1/4}\right).$$

We need to prove that the above asymptotic formula holds true if we replace $\widetilde{E}_G(k,d)$ by $E_G(k,d)$. First, it is clear by definition that

$$E'_G(k,d) := \widetilde{E}_G(k,d) \setminus E_G(k,d) = \bigcup_{H \text{ proper subgroup of} G} \widetilde{E}_H(k,d).$$

From the asymptotic formula (8)

$$\#E'_G(k,d) \le \sum_{H \text{ proper subgroup of} G} \#\widetilde{E}_H(k,d) \ll \frac{1}{d}\cdot \#\widetilde{E}_G(k,d),$$

hence we have

$$\#E_G(k,d) = \widetilde{E}_G(k,d)\left(1+O(d^{-1})\right).$$

Therefore

$$\frac{1}{\#E_G(k,d)} \sum_{\mathbb{K}\in\widetilde{E}_G(k,d)} \prod_{j=1}^{t} a_{\rho_j}(\mathbb{K})^{r_j} = \prod_{j=1}^{t} \frac{\delta(r_j)(r_j)!}{2^{r_j/2}\,(r_j/2)!} + O\left((\log l\beta)^{-1/4}\right).$$

Now we estimate

$$B = \frac{1}{\#E_G(k,d)} \sum_{\mathbb{K}\in E'_G(k,d)} \prod_{j=1}^{t} a_{\rho_j}(\mathbb{K})^{r_j}.$$

We find from (27) that

$$\begin{aligned} |B| &\le \sum_{H \text{ proper subgroup of } G} \left\{\frac{\#\widetilde{E}_H(k,d)}{\#E_G(k,d)}\right\} \frac{1}{\#\widetilde{E}_H(k,d)} \sum_{\mathbb{K}\in\widetilde{E}_H(k,d)} \prod_{j=1}^{t} a_{\rho_j}(\mathbb{K})^{r_j} \\ &\ll d^{-1}. \end{aligned}$$

Thus we obtain

$$\frac{1}{\#E_G(k,d)}\sum_{\mathbb{K}\in E_G(k,d)}\prod_{j=1}^{t} a_{\rho_j}(\mathbb{K})^{r_j}=\prod_{j=1}^{t}\frac{\delta(r_j)(r_j)!}{2^{r_j/2}\,(r_j/2)!}+O\left((\log l\beta)^{-1/4}\right).$$

This shows that the value $\left(a_{\rho_j}(\mathbb{K})\right)_{j=1}^{t}$ as $\mathbb{K}$ runs through $E_G(k,d)$ with $d\to\infty$ converges weakly to t independent standard Gaussian distributions. The completes the proof of Theorem 2. □

Theorem 1 can be derived from Theorem 2 as follows: first notice that

$$N_{\mathbf{I}}(\mathbb{K})=\sum_{1\neq\rho\in\widehat{G}}N_{\rho,\mathbf{I}}(\mathbb{K})+O(1),\tag{28}$$

where the term $O(1)$ comes from zeros of $\zeta_k(s)$. We choose a subset $A\subset\widehat{G}\setminus\{1\}$ with the property that for any $1\neq\rho\in\widehat{G}$, then

$$\#\left(\left\{\rho,\rho^{-1}\right\}\bigcap A\right)=1.$$

Obviously A exists and there are many choices for A. Then (28) can be written as

$$N_{\mathbf{I}}(\mathbb{K})=\sum_{\rho\in A}\epsilon_\rho N_{\rho,\mathbf{I}}(\mathbb{K})+O(1),$$

where

$$\epsilon_\rho=\begin{cases}1 & : \quad \text{if } \rho^2=1;\\ 2 & : \quad \text{if } \rho^2\neq 1.\end{cases}$$

This is because if $\rho^2\neq 1$, then $\rho\neq\rho^{-1}$ and $N_{\rho,\mathbf{I}}(\mathbb{K})=N_{\rho^{-1},\mathbf{I}}(\mathbb{K})$ for symmetry. We also have

$$N_{\mathbf{I}}(\mathbb{K})-g_{\mathbb{K}}\beta=\sum_{\rho\in A}\epsilon_\rho\left(N_{\rho,\mathbf{I}}(\mathbb{K})-m_{\rho,\mathbb{K}}\beta\right)+O(1).$$

From Theorem 2, as $\mathbb{K}$ runs through $E_G(k,d)$ with $d \to \infty$, the value $N_{\rho,\mathbf{I}}(\mathbb{K}) - m_{\rho,\mathbb{K}}\beta$ converges weakly to independent Gaussian distributions with mean zero and variance $\frac{r_\rho}{\pi^2}\log(l\beta)$ for all $\rho \in A$. So $N_{\mathbf{I}}(\mathbb{K}) - g_{\mathbb{K}}\beta$ also converges to a Gaussian distribution with mean zero. The variance is

$$\sigma^2 \quad \sim \quad \sum_{\rho\in A} \epsilon_\rho^2 \cdot \frac{r_\rho}{\pi^2}\log(l\beta) = \sum_{\rho\in A,\rho^2=1} \frac{2}{\pi^2}\log(l\beta) + \sum_{\rho\in A,\rho^2\neq 1} \frac{4}{\pi^2}\log(l\beta).$$

It is easy to see that the right hand side is

$$\sum_{\rho\in\widehat{G}\setminus\{1\},\rho^2\neq 1} \frac{2}{\pi^2}\log(l\beta) + \sum_{\rho\in\widehat{G},\rho^2\neq 1} \frac{2}{\pi^2}\log(l\beta) \quad = \quad \frac{2(\kappa-1)}{\pi^2}\log(l\beta),$$

where $\kappa = \#G$. We can also replace l by $g_{\mathbb{K}}$ since

$$\log(l\beta) \sim \log(g_{\mathbb{K}}\beta).$$

This completes the proof of Theorem 1. □

References

[1] A. Bucur, C. David, B. Feigon, M. Lalín, *Statistics for traces of cyclic trigonal curves over finite fields*, Int. Math. Res. Not. IMRN (2010), No. 5, 932–967.

[2] A. Bucur, C. David, B. Feigon, M. Lalín, *Fluctuations in the number of points on smooth plane curves over finite fields*, J. Number Theory **130** (2010), no. 11, 2528–2541.

[3] A. Bucur, C. David, B. Feigon, M. Lalín, *Biased statistics for traces of cyclic p-fold covers over finite fields*, WINŮwomen in numbers, 121–143, Fields Inst. Commun., **60**, Amer. Math. Soc., Providence, RI, 2011.

[4] A. Bucur, C. David, B. Feigon, M. Lalín, K. Sinha, *Distribution of zeta zeroes of Artin-Schreier curves*, to appear in Math. Res. Lett.

[5] A. Bucur, K. Kedlaya, *The probability that a complete intersection is smooth*, J. Theor. Nombres Bordeaux **24** (2012), no. 3, 541–556.

[6] P. Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–307.

[7] A. Entin, *On the distribution of zeroes of Artin-Schreier L-functions*, Geom. Funct. Anal. **22** (2012), 1322–1360.

[8] D. Faifman, Z. Rudnick, *Statistics of the zeros of zeta functions in families of hyperelliptic curves over a finite field*, Compos. Math. **146** (2010), no. 1, 81–101.

[9] N. M. Katz, P. Sarnak, "Random Matrices, Frobenius Eigenvalues, and Monodromy", Amer. Math. Soc. Colloq. Publ., vol. 45, American Mathematical Socitey, Providence, RI, 1999.

[10] P. Kurlberg, Z. Rudnick, *the fluctuations in the number of points on a hyperelliptic curve over a finite field*, J. Number Theory **129** (2009), no. 3, 580–587.

[11] P. Kurlberg, I. Wigman, *Gaussian point count statistics for families of curves over a fixed finite field*, Int. Math. Res. Not. IMRN 2011, no. 10, 2217–2229.

[12] H. L. Montgomery, "Ten lectures on the interface between analytic number theory and harmonic analysis". CBMS Regional Conference Series in Mathematics, **84**. American Mathematical Society, Providence, RI, 1994.

[13] C. Moreno, "Algebraic curves over finite fields", Cambridge Tracts in Mathematics **97**, Cambridge University Press, 1991.

[14] J. Neukirch, "Algebraic Number Theory". Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder. Grundlehren der Mathematischen Wissenschaften (Fundamental Principles of Mathematical Sciences), **322**. Springer-Verlag, Berlin, 1999.

[15] M. Rosen, "Number theory in function fields". Graduate Texts in Mathematics, **210**. Springer-Verlag, New York, 2002.

[16] M.J. Taylor, *On the equidistribution of Frobenius in cyclic extensions of a number field*, J. London Math. Soc. **29** (1984), no. 2, 211–223.

[17] A. Weil, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann et Cie., Paris, 1948.

[18] M.M. Wood, *The distribution of the number of points on trigonal curves over* $\mathbb{F}_q$, Int. Math. Res. Not. IMRN 2012, doi: 10.1093/imrn/rnr256.

[19] M.M. Wood, *On the probabilities of local behaviors in abelian field extensions*, Compos. Math. **146** (2010), no. 1, 102–128.

[20] D. Wright, *Distribution of discriminants of abelian extensions*, Proc. London Math. Soc. (3) **58** (1989), no. 1, 17–50.

[21] M. Xiong, *Statistics of the zeros of zeta functions in a family of curves over a finite field*, Int. Math. Res. Not. IMRN 2010, no. 18, 3489–3518.